

现代数学译丛

局部类域论

高维康 著

科学出版社

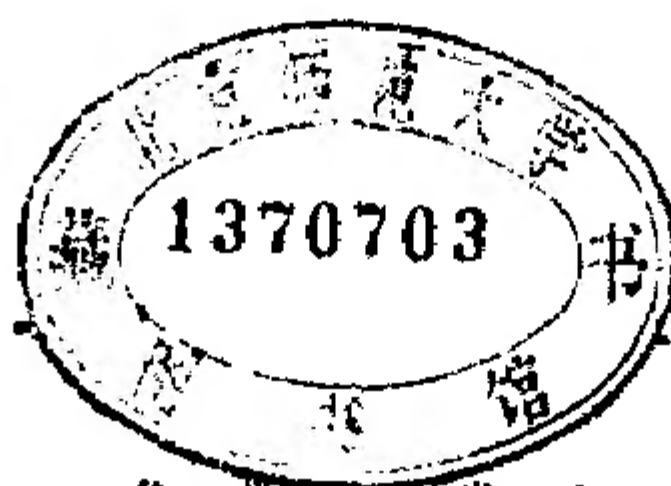
现代数学译丛

局部类域论

岩泽健吉 著

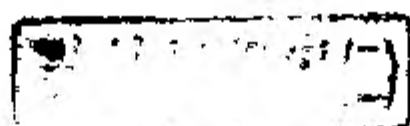
冯克勤 译

241154/23



科学出版社

1986



内 容 简 介

局部类域论是研究局部域 Abel 扩张的理论,是代数数论的一个重要组成部分,本书前三章介绍了完备域特别是局部域的一般理论,第四章以最大不分歧扩张为中心叙述了局部域无限扩张的理论,第五、六章为本书的核心,介绍局部类域论的主要结果,第七章是形式群在局部类域论中的应用,第八章考查了一个典型例子:局部分圆域.在附录中扼要叙述了 Hrauer 群和上同调方法.本书以初等方法和不大的篇幅叙述了局部类域论的基本内容,成为学习这一理论的一本极好的人门书.本书的英、俄译本均已出版.

本书可作为代数专业研究生的教材,是从事代数学(特别是代数数论)的研究人员和教学人员的有益参考书.

岩 澤 健 吉
局 所 類 体 論
岩波書店, 1980

现代数学译丛
局 部 类 域 论

岩泽健吉 著
冯克勤 译

责任编辑 杜小杨

科学出版社出版

北京朝阳门内大街137号

中国科学院印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1986年8月第 一 版	开本: 850×1168 1/32
1986年8月第一次印刷	印张: 5 1/2
印数: 0001—3,000	字数: 112,000

统一书号: 13031·3296

本社书号: 4942·13—1

定 价: 1.60 元

前 言

大家知道, Hilbert-高木-Artin 所发展的类域论 (Klassenkörpertheorie) 是关于代数数域和代数函数域的代数扩张、特别是 Abel 扩张的理论, 而局部类域论则是关于局部域扩张的同样的理论. 本书是从初等的观点讲述局部类域论的一般性入门书.

关于局部类域论, 无论是以它的理论自身为主题, 还是作为整体类域论的一部分, 目前在日本和其他国家都有不少优秀的著作. 对于前一种例如可以举出 Artin [1] 和 Serre [11], 而后一种则有 Cassels-Fröhlich [3], 彌永 [7], 河田 [8], Weil [14] 等. 这一理论有许多基本定理. 本书在讲述这一理论的时候, 固然仍以证明这些定理作为主要目标, 但是通往这一目标的途径, 即在证明方法上却与以往著作有许多相异之处. 现说明如下.

历史上, 局部类域论是由原来的整体类域论派生出来的. 所以起初前者的主要结果均可由后一理论推导出来. 但是随后出现了独立地构造局部类域论自身的方法 (十九世纪三十年代), 从而将局部类域论应用到整体类域论的证明之中. 后来从 1950 年前后, 开始了以 Hochschild 和中山为先驱的研究工作, 伴随着群的上同调理论的发展, 从更加广泛而透彻的观点给出局部类域论的证明. 前面所例举的著作几乎全是用了上同调方法 (但是仔细说来, Weil [14] 是建立在结合代数理论的基础上, 然而从结合代数中也可以看到上同调理论的来源). 直到最近, 荷兰数学家 M. Hazewinkel^[4] 发表了不用上同调群构造局部类域论的新方法. 概括地说, 如果把上同调方法看作是代数的乃至是群论的方法, 那末新的方法可以说成是数论的乃至是域论的方法. 因此, 采用这种新的方法, 特别是对于初学这一理论的人来说, 或许更易于理解局部类域论的数论内容.

本书主要是基于 Hazewinkel 的新构思来介绍局部类域论的概要。至于各章的内容,在每章开头都有一个概括的叙述,这里仅作一简单介绍。第一章至第三章对于完备域特别是局部域作了一般性的介绍,为后面几章作准备。第四章是局部域的基本理论,以最大不分歧扩张为主题讲述局部域的无限扩张。第五章和第六章是本书的核心与主要部分,在这里介绍 Hazewinkel 思想的一般化形式,由此证明局部类域论的主要结果。第七章介绍形式群在局部域上的应用,特别是用形式群给出存在定理的另一证明。最后在第八章,作为局部域的一个例子来考查局部分圆域,这一章的最后是证明关于范剩余符号的 Artin-Hasse 优美公式。

以上是本书的内容概要。作者在写作过程中以向读者传授知识作为主要目标,尽量避免运用对于局部类域论基本结果来说是多余的那些预备知识,虽然这样有时会走一些弯路。Hazewinkel 的方法正是以上述目的作为考虑的出发点。但是这样一来,本书中便没有机会接触到局部域上 Brauer 群理论。所以另外又加了一个附录,对于 Brauer 群作一简单介绍,同时也介绍了一点上同调方法。即使对于同一个数学分支,为了对精密而深刻的理论本身有更好的理解,在许多场合都有必要研究各种不同的方法和观点。局部类域论与原来的整体类域论比较起来虽然简单一些,但是仍旧有上述的必要性。本书作为一本入门书,展示出局部类域论的一条通路。作者希望读者能以本书为出发点,然后从关于这一理论的其他著作中学习别的方法,进而把研究领域扩大到整体类域论中去。

如上所述,本书不需要很多预备知识。只需要代数学、拓扑空间理论和拓扑群论的一般性基础知识就可以理解本书的内容。此外,在叙述过程中还有一些引伸出来的话题,在这些地方读者可根据所列文献自行补足。引用的文献表附在书末。关于局部域和局部类域论的详细文献可见 Serre [11]。

著 者

1979 年 5 月

目 录

前言	
第一章 完备域	1
§ 1.1 赋值	1
§ 1.2 赋值的限制、扩充和完备化	3
§ 1.3 完备域	7
§ 1.4 完备域的 Galois 扩域	13
第二章 闭完备域	17
§ 2.1 范映射	17
§ 2.2 基本正合序列	22
第三章 局部域	27
§ 3.1 局部域的一般性质	27
§ 3.2 有限扩域	32
§ 3.3 局部域的范群	35
第四章 极大不分歧扩域	41
§ 4.1 代数扩域和它的范群	41
§ 4.2 极大不分歧扩域 k_{ur}	44
§ 4.3 $K = k_{ur}$ 的扩域	50
第五章 Abel 扩张 k_{ab}/k_{ur}	55
§ 5.1 有限 Galois 扩张 E/k	55
§ 5.2 $\mathcal{G}_{E/k}$ 的性质	62
§ 5.3 拓扑同构 \mathcal{G}_k	71
第六章 基本定理	80
§ 6.1 基本映射 ρ_A	80
§ 6.2 ρ_A 的性质	84
§ 6.3 有限 Abel 扩域	92
第七章 形式群及其应用	100

§ 7.1 一般的形式群	100
§ 7.2 形式群 $F_r(X, Y)$	101
§ 7.3 Abel 扩域 k_∞	108
第八章 局部分圆域	120
§ 8.1 局部分圆域	120
§ 8.2 范剩余符号	128
§ 8.3 局部域上的微分	136
§ 8.4 Artin-Hasse 公式	140
附录 局部域的 Brauer 群	153
§ A.1 一般的上同调群	153
§ A.2 Galois 群的上同调群	158
§ A.3 局部域的 Brauer 群	162
参考文献	169

第一章 完 备 域

作为准备,本章开始介绍关于完备正规赋值域的基本结果,但是对于一般的代数教科书(例如藤崎[5], van der Waerden [13]等)中包含的一些事实,这里省略了证明. 详情还请参考专门的赋值论书籍以及 Artin [1], 彌永[7], Serre [11]等.

§ 1.1 赋 值

定义在域 k 上的函数 $v(x) (x \in k)$, 如果满足下列诸条件, 便叫作 k 的(指数)赋值:

i) $v(0) = +\infty$; 而当 $x \neq 0$ 时 $v(x)$ 是实数;

ii) 对于任意的 $x, y \in k$,

$$\min(v(x), v(y)) \leq v(x+y);$$

iii) 对于任意的 $x, y \in k$,

$$v(x) + v(y) = v(xy).$$

由定义立即得出

$$v(\pm 1) = 0; v(x) = v(-x); v(x) < v(y) \Rightarrow v(x+y) = v(x).$$

其中 $1 = 1_k$ 是 k 的单位元素. 此外, 如果令

$$\mathfrak{o} = \{x \in k \mid v(x) \geq 0\},$$

$$\mathfrak{p} = \{x \in k \mid v(x) > 0\},$$

则 \mathfrak{o} 是 k 的子环而 \mathfrak{p} 是 \mathfrak{o} 的极大理想. 从而

$$\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$$

是域. \mathfrak{o} , \mathfrak{p} 和 \mathfrak{f} 分别叫作 v 的赋值环, 极大理想和剩余类域. 由定义中的 iii) 可知 v 定义出从域 k 的乘法群 k^\times 到实数加法群 \mathbf{R}^+ 中的同态

$$v: k^\times \rightarrow \mathbf{R}^+.$$

从而 $v(k^\times)$ 是 R^+ 的子群, 如果令

$$U = \text{Ker}(v) = \{x \in k \mid v(x) = 0\},$$

则有自然同构

$$k^\times/U \cong v(k^\times),$$

我们把 U 叫作 v 的单位群.

设 v 为 k 的赋值. 对于任意正实数 $\alpha > 0$, 定义

$$v'(x) = \alpha v(x), \quad x \in k,$$

则 v' 显然也是 k 的赋值. 当 k 的两个赋值 v 和 v' 满足这样的关系, 即一个为另一个的正数倍时, 我们写成

$$v \sim v',$$

并且称它们是等价的赋值. 等价的赋值具有相同的赋值环、极大理想和剩余类域, 还有许多其他共同的性质.

设 k 和 v 如上所述, 给了一个固定的实数 β , $0 < \beta < 1$, 对于 k 中任意元素 x 和 y , 令

$$\rho(x, y) = \beta^{v(x-y)},$$

ρ 定义出 k 上一个距离, 由此 k 是距离空间, 从而也是 Hausdorff 拓扑空间. 取不同的 β 值, 则对应的距离 ρ 是彼此等价的, 所以 k 上由 ρ 给出的拓扑是不变的. 也就是说, 该拓扑由赋值 v 所唯一决定. 不难看出, k 对于这一拓扑是拓扑域. 如果 k 对于上述的距离 ρ 是完备距离空间的时候, 我们称 v 是 k 的完备赋值. 注意当 β 改变从而 ρ 改变时, 其完备性是不变的. 此外, 如果 $v \sim v'$, 则 v 和 v' 在 k 上定义出等价的距离, 特别地, 如果 v 是完备的, 则 v' 也是完备的.

继续设 v 是 k 的赋值. 如果 R^+ 的子群 $v(k^\times)$ 是有理整数加法群, 即

$$v(k^\times) = \mathbf{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\},$$

则将 v 叫作 k 的正规赋值. 这时取 k 中元素 π 使得

$$v(\pi) = 1,$$

这样的 π 叫作正规赋值 v 的素元. 对于一个确定的素元 π , 由于 $\mathfrak{p} = \{x \in k \mid v(x) \geq 1\}$, 从而得到

$$\mathfrak{p} = (\pi) = 0\pi.$$

于是 \mathfrak{p} 的方幂为

$$\mathfrak{p}^n = (\pi^n) = 0\pi^n = \{x \in k \mid v(x) \geq n\}, \quad n \geq 0.$$

由于 $v(x) \geq n$ 和 $v(x) > n-1$ 是一回事, 所以 $\mathfrak{p}^n (n \geq 0)$ 均是 k 的开(加法)子群. 并且不难看出, 对于由上述的 v 所定义的 k 的拓扑, $\{\mathfrak{p}^n\}_{n \geq 0}$ 形成 0 的基本邻域系. 也就是说, 由 v 决定的 k 的拓扑是 p -adic 拓扑. 注意 \mathfrak{p}^n 是 k 的开子群, 从而也是闭子群. 由于 $\mathfrak{p}^n = (\pi^n) \ni \{0\}$, 所以拓扑域 k 是全不连通的, 但不是离散的.

仍令 v 为 k 的正规赋值, 但是这次考虑 k 的乘法群 k^\times . 由前述的同构 $k^\times/U \xrightarrow{\sim} v(k^\times) = \mathbb{Z}$ 可得

$$k^\times = \langle \pi \rangle \times U, \quad \langle \pi \rangle \cong \mathbb{Z}.$$

其中 $\langle \pi \rangle$ 是由素元 π 生成的 k^\times 的子群. 此外, 若令

$$U_0 = U, \quad U_n = 1 + \mathfrak{p}^n = 1 + 0\pi^n, \quad n \geq 1,$$

不难看出它们均是 k^\times 的子群, 并且

$$\cdots \subseteq U_{n+1} \subseteq U_n \subseteq \cdots \subseteq U_1 \subseteq U_0 = U \subseteq k^\times.$$

k^\times 对于由 k 的 p -adic 拓扑所诱导的拓扑是 Abel 拓扑群, 并且 U_n 均是它的开子群, 而且由上述的内容可知 $\{U_n\}_{n \geq 0}$ 形成 k^\times 中 1 的基本邻域系. 进而, 如果以 \mathfrak{f}^+ 和 \mathfrak{f}^\times 分别表示剩余类域 $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ 的加法群和乘法群, 则有

$$U_0/U_1 \cong \mathfrak{f}^\times, \quad U_n/U_{n+1} \cong \mathfrak{f}^+, \quad n \geq 1.$$

实际上不难看出, 自然满同态 $\mathfrak{o} \rightarrow \mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ 给出乘法群的满同态 $U = U_0 \rightarrow \mathfrak{f}^\times$, 然后由此即得到 $U_0/U_1 \cong \mathfrak{f}^\times$. 而当 $n \geq 1$ 的时候, $U_n = 1 + 0\pi^n$ 中的元素均可写成 $1 + x\pi^n$, $x \in \mathfrak{o}$, 则由 $1 + x\pi^n \bmod U_{n+1} \mapsto x \bmod \mathfrak{p}$ 即得出 $U_n/U_{n+1} \cong \mathfrak{f}^+$.

§ 1.2 赋值的限制、扩充和完备化

设 k' 是 k 的任意扩域而 μ 为 k' 的赋值, 函数 μ 在子域 k 上的限制记成 $\mu|_k$, 它显然是 k 的赋值, 叫作 μ 在子域 k 上的限制. 另

一方面,对于 k 的赋值 ν 如果存在 k' 上的赋值 μ 使得

$$\mu|_k = \nu,$$

则 μ 叫作 ν 到扩域 k' 的扩充. 对于 k' 上的赋值 μ , 它的限制 $\mu|_k$ 是唯一确定的. 反过来, 给了 k 的赋值 ν , 是否存在 ν 到 k' 上的扩充 μ , 并且若存在是否唯一, 这是赋值论的一个重要问题.

如上令 $\mu|_k = \nu$. 由 ν 给出的 k 的拓扑显然是由 μ 所给出的 k' 的拓扑所诱导出来的. 也就是说, 作为拓扑域, k 是 k' 的子域. 设 μ 的赋值环、极大理想和剩余类域分别为

$$\mathfrak{o}' = \{x' \in k' \mid \mu(x') \geq 0\},$$

$$\mathfrak{p}' = \{x' \in k' \mid \mu(x') > 0\},$$

$$\mathfrak{f}' = \mathfrak{o}'/\mathfrak{p}',$$

则由定义立刻知道

$$\mathfrak{p} = \mathfrak{o} \cap \mathfrak{p}'.$$

因而

$$\mathfrak{f} = \mathfrak{o}/\mathfrak{p} = \mathfrak{o}/\mathfrak{o} \cap \mathfrak{p}' = (\mathfrak{o} + \mathfrak{p}')/\mathfrak{p}' \subseteq \mathfrak{o}'/\mathfrak{p}' = \mathfrak{f}'.$$

也就是说, 可以把 k 的剩余类域 \mathfrak{f} 自然地看成是 k' 的剩余类域 \mathfrak{f}' 的子域. 另一方面, 由 $\mu|_k = \nu$ 知道

$$\nu(k^\times) \subseteq \mu(k'^\times) \subseteq \mathbf{R}^+.$$

定义群指数和域的扩张次数分别为

$$e = [\mu(k'^\times); \nu(k^\times)], \quad f = [\mathfrak{f}': \mathfrak{f}].$$

其中 e, f 为自然数 $1, 2, 3, \dots$, 或者是 $+\infty$. 我们将

$$e = e(\mu/\nu), \quad f = f(\mu/\nu)$$

叫作 μ/ν 的分歧指数和剩余类次数.

作为赋值扩充的一个例子, 我们来叙述关于完备化的熟知结果¹⁾. 设给了域 k 的赋值 ν , 则存在 k 的扩域 k' 以及 ν 到 k' 上的扩充 μ 满足如下两个条件: 1) μ 是 k' 的完备赋值; 2) 对于由 μ 决定的 k' 的拓扑, k 是 k' 的稠子集. 这样的 k' , 或者更确切地说, 由

1) 关于完备化的一般理论可参见藤崎[7]第六章, 或者 v. d. Waerden [13], 第十章.

k' 和 μ 组成的 (k', μ) 叫作 k 的赋值 ν 的完备化. 如果 (k', μ) 和 (k'', ω) 均是 ν 的完备化, 则存在 k 同构 $\sigma: k' \xrightarrow{\sim} k''$ 使得 $\mu = \omega \circ \sigma$. 因此, 完备化本质上是唯一确定的. 此外, 对于 k' 中任意元素 x' , 由 2) 可知存在 $x_n \in k$, 使得 $x' = \lim_{n \rightarrow \infty} x_n$, 从而

$$\mu(x') = \lim_{n \rightarrow \infty} \nu(x_n).$$

由此即知

$$e(\mu/\nu) = f(\mu/\nu) = 1.$$

也就是说

$$\nu(k^x) = \mu(k'^x), \quad f' = f.$$

完备化的重要性在于, 完备赋值具有许多 (一般赋值不具备的) 特别的性质. 例如下面所述的著名的 Hensel 引理成立¹⁾.

引理 1 假设 ν 是域 k 的完备赋值, $f = a/p$ 是 k 的剩余类域. $f(X)$, $g_0(X)$ 和 $h_0(X)$ 均是多项式环 $\mathfrak{o}[X]$ 中的多项式, 并且满足

$$f(X) \equiv g_0(X)h_0(X) \not\equiv 0 \pmod{p}.$$

如果 $g_0(X) \pmod{p}$ 和 $h_0(X) \pmod{p}$ 是 $\mathbb{F}[X]$ 中互素的多项式, 则存在 $\mathfrak{o}[X]$ 中的多项式 $g(X)$ 和 $h(X)$ 满足下列条件:

$f(X) = g(X)h(X)$, $g(X) \equiv g_0(X) \pmod{p}$, $h(X) \equiv h_0(X) \pmod{p}$, 并且 $g(X)$ 的次数等于 $g_0(X) \pmod{p}$ 的次数.

上面的 Hensel 引理是赋值论的基本工具, 它有许多应用, 下面的引理便是其中之一.

引理 2 假设 k' 是 k 的代数扩域, 则 k 的完备赋值 ν 可以唯一地扩充成 k' 上的赋值. 又如果 k'/k 是有限扩张, 则 μ 也是完备赋值. 又若 $n = [k':k]$, 并以 $N_{k'/k}$ 表示 k'/k 的范, 则对 k' 中任意元素 x' 均有

$$\mu(x') = \frac{1}{n} \nu(N_{k'/k}(x')).$$

引理 3 设 k', k , ν 和 μ 如引理 2 所述, 又设 σ 是 k' 的 k 自

1) 关于引理 1 和 2 的证明参见第 4 页脚注 1) 中的文献.

同构, 则 $\mu \circ \sigma = \mu$, 即

$$\mu(\sigma(x')) = \mu(x'), \quad x' \in k'.$$

从而 $\sigma: k' \xrightarrow{\sim} k'$ 对于由 μ 定义的拓扑是 k' 的拓扑自同构. 此外, 若以 $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ 和 $\mathfrak{f}' = \mathfrak{o}'/\mathfrak{p}'$ 分别表示 ν 和 μ 的剩余类域, 则

$$\sigma(\mathfrak{o}') = \mathfrak{o}', \quad \sigma(\mathfrak{p}') = \mathfrak{p}'.$$

从而 σ 诱导出 \mathfrak{f}' 的 \mathfrak{f} -自同构

$$\sigma': \mathfrak{f}' \xrightarrow{\sim} \mathfrak{f}.$$

证明 令 $\mu' = \mu \circ \sigma$, 易知 μ' 是 k' 的赋值. 对于 $x \in k$, 则 $\mu'(x) = \mu(\sigma(x)) = \mu(x) = \nu(x)$, 即 μ' 也是 ν 到 k' 上的扩充. 由引理 2 关于扩充的唯一性可知 $\mu' = \mu$, 即 $\mu \circ \sigma = \mu$. 后一部分的论断是显然的.

引理 4 设 k'/k , ν , μ , \mathfrak{o} 和 \mathfrak{o}' 如引理 3 所示, 则 \mathfrak{o}' 是 \mathfrak{o} 在 k' 中的整闭包. 又若 k'/k 是有限扩张, 则迹映射和范映射

$$T_{k'/k}, N_{k'/k}: k' \rightarrow k$$

对于由 ν 和 μ 所定义的拓扑均是连续映射.

证明 设 x' 为 k' 中任意元素, 则 $k(x')/k$ 为有限扩张, 从而对于前半部分的推断只需对 k'/k 是有限扩张的情形加以证明即可. 令 $[k':k] = n$ 而 Ω 是 k' 的代数闭包, 则恰好存在 n 个 k 单同态 $k' \rightarrow \Omega$ (重复的考虑在内), 设它们是 $\sigma_1, \dots, \sigma_n$, 而对于 k' 中任意元素 x' , 令

$$\prod_{i=1}^n (X - \sigma_i(x')) = X^n + a_1 X^{n-1} + \dots + a_n, \quad a_i \in k.$$

a_1, a_2, \dots, a_n 均是 $\sigma_1(x'), \dots, \sigma_n(x')$ 的对称多项式. 特别地,

$$a_1 = - \sum_{i=1}^n \sigma_i(x') = -T_{k'/k}(x'),$$

$$a_n = (-1)^n \prod_{i=1}^n \sigma_i(x') = (-1)^n N_{k'/k}(x').$$

每个 σ_i 都可以扩充成 Ω 的 k 自同构, 又由引理 2 知道 μ 可以扩充成 Ω 的赋值 μ' , 而由引理 3 知道 σ_i 对于由 μ' 决定的拓扑是 Ω 的

拓扑自同构,从而由上面等式可知 $T_{k'/k}$ 和 $N_{k'/k}$ 均是连续映射.其次设 $x' \in \mathfrak{o}$, 即 $\mu(x') \geq 0$, 则由引理 3 可知

$$\mu'(\sigma_i(x')) = \mu'(x') = \mu(x') \geq 0, \quad 1 \leq i \leq n.$$

从而 $\nu(a_i) = \mu'(a_i) \geq 0$, 即 $a_i \in \mathfrak{o}$, $1 \leq i \leq n$. 因此 x' 对于 \mathfrak{o} 是整元,反之,假设 x' 对于 \mathfrak{o} 是整元,则有

$$x'^m + b_1 x'^{m-1} + \cdots + b_m = 0, \quad b_i \in \mathfrak{o},$$

于是 $\mu(b_i) = \nu(b_i) \geq 0$ ($1 \leq i \leq m$), 从而 $\mu(x') \geq 0$, 即得到 $x' \in \mathfrak{o}$.

从上面的引理 4 可知, 赋值环 \mathfrak{o} 在 k 中是整闭的. 此外根据上面的证明知道, 如果 $x' \in \mathfrak{p}'$, 则 $\mu'(\sigma_i(x')) = \mu'(x') > 0$, 从而得到

$$\nu(a_i) = \mu'(a_i) > 0, \quad \text{即 } a_i \in \mathfrak{p} \quad (1 \leq i \leq n).$$

特别地,

$$T_{k'/k}(\mathfrak{p}'), N_{k'/k}(\mathfrak{p}') \subset \mathfrak{p}.$$

§ 1.3 完 备 域

通常在习惯上把具有完备赋值 ν 的域 k 叫作完备域. 而在本书中为方便起见, 今后则只限于对 ν 是完备正规赋值的情形, 称域 k 是(具有赋值 ν 的)完备域. 更确切地, 对于一个完备域, 应当将域 k 和其上的完备正规赋值 ν 放在一起而表示成 (k, ν) . 在 §1.1 中对于赋值 ν 所定义的 \mathfrak{o} , \mathfrak{p} , $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$, U 等分别叫作完备域 (k, ν) 的或者简称作 k 的赋值环, 极大理想, 剩余类域和单位群. 此外, 正规赋值 ν 的素元 π 也叫作 k 的素元.

设 ν 是域 k 的任意正规赋值, (k', ν') 是 k 中赋值 ν 的完备化, 则由上节可知 $\nu'(k'^{\times}) = \nu(k^{\times}) = \mathbb{Z}$, 从而 ν' 是完备的正规赋值, 因而 (k', ν') 是完备域. 由此可以得到许多完备域的自然例子.

例 1 设 p 为任意素数, ν 是有理数域 Q 上熟知的 p -adic 赋值, 则 Q 对于 ν 的完备化即是 p -adic 数域 Q_p . 由于 ν 是正规赋

值,从上面的注记可知 \mathbf{Q}_p 是完备域. \mathbf{Q}_p 的赋值环为 p -adic 整数环 \mathbf{Z}_p , 极大理想是 $p\mathbf{Z}_p$, 从而剩余类域为 $\mathbf{Z}_p/p\mathbf{Z}_p$, 即是由 p 个元素组成的有限域 \mathbf{F}_p .

例 2 设 F 是任意域. 令 $F((X))$ 为所有系数属于 F 并且至多有有限个负幂项的形式幂级数

$$\sum_{-\infty < n} a_n X^n, \quad a_n \in F$$

所组成的集合, 则 $F((X))$ 是 F 的扩域. 设 a_{n_0} 是上面幂级数中第一个不是 0 的系数, 定义

$$v\left(\sum_{-\infty < n} a_n X^n\right) = n_0$$

(而令 $v(0) = +\infty$), 则 v 是 $F((X))$ 的完备正规赋值. (读者自行证明 v 实际上是完备的.) 从而 $(F((X)), v)$ 是完备域. $F((X))$ 的赋值环为整幂级数全体 $F[[X]]$, 极大理想是 $(X) = XF[[X]]$, 从而剩余类域为 $F[[X]]/XF[[X]] = F$. $F((X))$ 包含有理函数域 $F(X)$. v 的限制 $v|_{F(X)}$ 是 $F(X)$ 的正规赋值, 它是由多项式环 $F[X]$ 的素理想 $XF(X)$ 所定义的 (就象 \mathbf{Q} 上的 p -adic 赋值一样). 从而 $(F((X)), v)$ 不过是 $F(X)$ 对于 $v|_{F(X)}$ 的完备化.

设 (k, v) 是任意完备域, 取 A 为它的剩余类域 $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ 在 \mathfrak{o} 中的完全代表系, 即 A 是 \mathfrak{o} 的一个子集合, 使得 $\mathfrak{o}/\mathfrak{p}$ 中每个剩余类在 A 中恰好有一个代表元. 并且取 k 中零元素 0 作为 $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ 中零元素即 \mathfrak{p} 的代表元. 令 π 为 k 中素元, 由于 v 是完备的, 从而形如

$$\sum_{-\infty < n} a_n \pi^n, \quad a_n \in A$$

的每个级数对于 p -adic 拓扑在 k 内都是收敛的, 即给出 k 中一个元素 x . 如果令 a_{n_0} 是上面级数中第一个不为 0 的系数, 则 $a_{n_0} \in \mathfrak{o}$, $a_{n_0} \notin \mathfrak{p}$, 于是 $v(a_{n_0}) = 0$, 由此不难得到

$$v(x) = n_{00}$$

定理 1 (展开定理) 设 A 和 π 如上所述, 则 k 中每个元素 x 均可以唯一地表示成以下形式:

$$x = \sum_{n \in \mathbb{N}} a_n \pi^n, \quad a_n \in A.$$

特别地,

$$\mathfrak{o} = \left\{ \sum_{n=0}^{\infty} a_n \pi^n \mid a_n \in A \right\}, \quad \mathfrak{p} = \left\{ \sum_{n=1}^{\infty} a_n \pi^n \mid a_n \in A \right\}.$$

证明 设 $x \neq 0$, $v(x) = v_0$, 则 $v(\pi^{-v_0}x) = 0$, 因此只需对于 $v(x) = 0$ 的情形证明定理即可. 假设 $x \in \mathfrak{o}$, 则存在 $a_0 \in A$ 使得 $x = a_0 \bmod \mathfrak{p}$. 由于 $x \notin \mathfrak{p}$ 从而 $a_0 \neq 0$. 由 $\mathfrak{p} = \mathfrak{o}\pi$ 可知 $x = a_0 + x'\pi$, $x' \in \mathfrak{o}$. 于是 $x' = a_1 \bmod \mathfrak{p}$, $a_1 \in A$, 从而 $x = a_0 + a_1\pi \bmod \mathfrak{p}^2$. 同样由 $\mathfrak{p}^2 = \mathfrak{o}\pi^2$ 可知 $x = a_0 + a_1\pi + x''\pi^2$, $x'' \in \mathfrak{o}$, 从而 $x = a_0 + a_1\pi + a_2\pi^2 \bmod \mathfrak{p}^3$. 由此决定出 A 中元素 a_0, a_1, a_2, \dots ,

显然 $x = \sum_{n=0}^{\infty} a_n \pi^n$. 从上面的证明过程不难看出 a_n 的唯一性 (参见下面系的证明). 此外由上面的公式 $v(x) = v_0$ 即给出关于 \mathfrak{o} 和 \mathfrak{p} 的等式.

系 集合 A 赋以离散拓扑, 并且将可数 $\wedge A$ 的积集合

$$A^{\infty} = \{(a_0, a_1, a_2, \dots) \mid a_n \in A\}$$

赋以积拓扑, 则映射

$$(a_0, a_1, a_2, \dots) \longrightarrow \sum_{n=0}^{\infty} a_n \pi^n$$

定义了一个从拓扑空间 A^{∞} 到 \mathfrak{o} 的一个同胚.

证明 设 $x = \sum_{n=0}^{\infty} a_n \pi^n$, $y = \sum_{n=0}^{\infty} b_n \pi^n$, $a_n, b_n \in A$. 则对于任意的 $i \geq 1$, 用数学归纳法不难证明

$$x \equiv y \bmod \mathfrak{p}^i \iff a_0 = b_0, a_1 = b_1, \dots, a_{i-1} = b_{i-1}.$$

从而由积拓扑的定义即可证明该系的论断.

注记 一般地对于每个整数 n , 均确定 k 中一个元素 π_n 满足

$v(\pi_n) \neq 0$, 则可以象定理 1 一样地证明, k 中任意元素 x 均可以唯一地表示成如下形式

$$x = \sum_{-\infty < n} a_n \pi_n, \quad a_n \in A.$$

而定理 1 则是 $\pi_n = \pi^n$ 这一特殊情形.

现在考查完备域的有限扩域.

定理 2 设 (k, v) 是完备域而 k' 是 k 的任意有限扩域, 则 k' 上存在唯一的正规赋值 v' 使得

$$v'|k \sim v.$$

并且 v' 是完备的, 从而 (k', v') 也是完备域.

证明 由 §1.2 中的引理 2 可知 v 可以唯一地扩充成 k' 的完备赋值 μ , 如果 $n = [k':k]$, 则

$$n\mu(k'^{\times}) \subseteq v(k^{\times}) = \mathbb{Z},$$

$$e = e(\mu/v) = [\mu(k'^{\times}) : v(k^{\times})] < +\infty.$$

因此, 若令

$$v' = e\mu,$$

则

$$v'(k'^{\times}) = \mathbb{Z}, \quad v'|k = ev \sim v.$$

从 v' 的扩充 μ 的唯一性可知 v' 的唯一性.

今后, 完备域 k 的有限扩域 k' 均看成是上述意义下(对于定理 2 中的赋值 v')的完备域. 令 $e = e(\mu/v)$, 则

$$v'|k = ev,$$

从而 $e = e(\mu/v)$ 是由 (k, v) 和 (k', v') 所唯一决定的, 称作扩张 k'/k 的分歧指数, 并且表示成

$$e(k'/k).$$

另一方面, 设 $\mathfrak{p} = \mathfrak{o}'/\mathfrak{p}'$ 是 (k', v') 的剩余类域, 则由 $v' \sim \mu$ 可知 \mathfrak{p} 也是 μ 的剩余类域. 由 §1.2 可知 $\mathfrak{p} \subseteq \mathfrak{p}'$, $f(\mu/v) = [\mathfrak{p}':\mathfrak{p}]$, 这里 $[\mathfrak{p}':\mathfrak{p}]$ 也是由完备域扩张 k'/k 所唯一决定的, 叫作 k'/k 的剩余类次数, 并且表示成

$$f(k'/k).$$

其次我们要证 $f(k'/k)$ 是有限的. 为此令 $\{\omega_1, \dots, \omega_s\}$ 是 $\mathfrak{f} = \mathfrak{o}'/\mathfrak{p}'$ 的有限子集合, 并且在 \mathfrak{f} 上是线性无关的. 在每个剩余类 $\omega_i (1 \leq i \leq s)$ 中取定一个 \mathfrak{o} 中的代表元 ξ_i . 假设有 k 中不全为零的元素 x_1, \dots, x_s , 使得

$$\sum_{i=1}^s x_i \xi_i = 0,$$

不妨设 $x_1 \neq 0$, 并且 $v(x_1) \leq v(x_i) (1 \leq i \leq s)$. 令 $y_i = x_i/x_1 (1 \leq i \leq s)$, 则 $\sum_{i=1}^s y_i \xi_i = 0$, $y_i \in \mathfrak{o}$, 并且 $y_1 = 1 \pmod{\mathfrak{p}}$ 之后 ω_1 便是 $\omega_1, \dots, \omega_s$ 的 \mathfrak{f} 线性组合, 这就与假设相矛盾. 从而 ξ_1, \dots, ξ_s 是 k -线性无关的, 于是 $s \leq n = [k':k]$. 于是得到 $f(k'/k) = [\mathfrak{f}:\mathfrak{f}] \leq n$.

定理 3 设 k'/k 如上所示, 令 $e = e(k'/k)$, $f = f(k'/k)$, $n = [k':k]$, 则

$$ef = n.$$

证明 设 $\omega_1, \dots, \omega_f$ 是 \mathfrak{f} 在 \mathfrak{f} 上的一组基, 象上面那样, 在每个剩余类 ω_i 中取定 \mathfrak{o}' 中一个代表元 ξ_i . 令 A 是定理 1 中所述的 $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ 的完全代表系, 则不难看出

$$A' = \left\{ \sum_{i=1}^f a_i \xi_i \mid a_i \in A \right\}$$

是 $\mathfrak{f} = \mathfrak{o}'/\mathfrak{p}'$ 的完全代表系并且 $0 \in A'$. 进而, 给定 k 的素元 π 和 k' 的素元 π' , 对于任意整数 $m = \iota e + j$, $\iota \in \mathbf{Z}, 0 \leq j < e$, 令

$$\pi_m = \pi'^j \pi'^{\iota},$$

则由 $v'(\pi) = e v(\pi) = e$ 可知 $v'(\pi_m) = m$. 根据定理 1 后面的注记可知 k' 中每个元素 x' 均可唯一地表示成

$$\sum_{-\infty < m} \alpha_m \pi_m, \alpha_m \in A'.$$

令 $\alpha_m = \sum_{i=1}^f a_{m,i} \xi_i$, $a_{m,i} \in A$, 则

$$x' = \sum_{i,j} x_{ij} \xi_i \pi'^j, \quad x_{ij} = \sum_l a_{l,j,i} \pi'^l \in k.$$

由此即知 $\xi_i \pi'^j (1 \leq i \leq f, 0 \leq j < e)$ 是 k'/k 的一组基. 特别有 $ef = n$.

系 设 (k', v') 如定理 2 所述, 则

$$v'(x') = \frac{1}{f} v(N_{k'/k}(x')), \quad x' \in k'.$$

证明 由 §1.2 中的引理 2 以及 $v' = e\mu$ 和 $n = ef$ 即可证明.

也可以用 k 和 k' 的素元 π 和 π' 的赋值表示出 $e = e(k'/k)$ 和 $f = f(k'/k)$. 从定理 3 的证明过程已经知道

$$e = v'(\pi).$$

另一方面, 在定理 3 的系中取 $x' = \pi'$, 则

$$f = v(N_{k'/k}(\pi')).$$

如果 k' 又有有限扩域 k'' , 则由定理 2 可知 k'' 也是完备域, 并且从定义直接得到

$$e(k'', k') = e(k''/k')e(k'/k), \quad f(k''/k) = f(k''/k')f(k'/k).$$

对于扩张 k'/k , 如果

$$e = 1, f = n,$$

则称 k'/k 为不分歧扩张, 而将 k' 叫作 k 的不分歧扩域¹⁾. 另一方面, 如果

$$e = n, f = 1,$$

则称 k'/k 为完全分歧扩张. 根据上面的注记可知, k'/k 是不分歧扩张的充要条件是 k 的素元 π 也是 k' 的素元. 另一方面, k'/k 是完全分歧扩张的充要条件是: 若 π' 为 k' 的素元, 则 $N_{k'/k}(\pi')$ 是 k 的素元. 并且对于后一情形则 $k' = k(\pi')$, 这是因为: 如果 $k' \neq k(\pi')$, 则 $v(N_{k'/k}(\pi')) \geq [k':k(\pi')] > 1$. 此外, 如果 k'/k 是完全分歧的, 则 $f = [f':f] = 1$, 即 $f' = f$, 从而 k 的剩余类域

1) Artin [1] 中在定义 k'/k 为不分歧扩张时, 除了 $e = 1$ 和 $f = n$ 之外, 还需要假定剩余类域扩张 f'/f 是可分的. 以后各章所研究的 k'/k , 其 f' 均是有限域, 从而 f', f 必然是可分扩张, 因此这两种定义是一回事.

$f = \mathfrak{o}/\mathfrak{p}$ 在 \mathfrak{o} 中的完全代表系 A 同时也是 k' 的剩余类域 $f' = \mathfrak{o}'/\mathfrak{p}'$ 在 \mathfrak{o}' 中的完全代表系. 因此若 π' 为 k' 的素元, 则由定理 1 可知

$$\mathfrak{o}' = \left\{ \sum_{n=0}^{\infty} a_n \pi'^n \mid a_n \in A \subset \mathfrak{o}' \right\}.$$

另一方面, 对于 \mathfrak{o} 中任意元素 $a_n (n \geq 0)$, $\sum_{n=0}^{\infty} a_n \pi'^n$ 必然在 \mathfrak{o}' 中收敛, 从而

$$\mathfrak{o}' = \mathfrak{o}[[\pi']] = \left\{ \sum_{n=0}^{\infty} a_n \pi'^n \mid a_n \in \mathfrak{o} \right\}.$$

(由此也可得出 $k' = k(\pi')$.)

§ 1.4 完备域的 Galois 扩域

仍设 (k, v) 为完备域, k' 是 k 的有限扩域. 本节中我们研究 k'/k 是 Galois 扩张的情形, 令 k'/k 的 Galois 群为

$$G = \text{Gal}(k'/k).$$

将 §1.2 中的引理 3 用于 G 中任意元素 σ , 可知 σ 诱导出剩余类域 $f' = \mathfrak{o}'/\mathfrak{p}'$ 以及一般的剩余类环 $\mathfrak{o}'/\mathfrak{p}'^{i+1} (i \geq 0)$ 上的自同构. 以 G_i 表示在 $\mathfrak{o}'/\mathfrak{p}'^{i+1}$ 上诱导出恒等映射的 G 中元素 σ 所构成的集合, 即

$$G_i = \{ \sigma \in G \mid \sigma(x') \equiv x' \pmod{\mathfrak{p}'^{i+1}}, \forall x' \in \mathfrak{o}' \}.$$

显然 G_i 是 G 的正规子群, 并且

$$\cdots \subseteq G_{i+1} \subset G_i \subseteq \cdots \subseteq G_1 \subseteq G_0 \subseteq G.$$

定理 4 设 k'/k 为完全分歧的 Galois 扩张, 则 $G = G_0$, 并且对于充分大的 i 有 $G_i = 1$. 此外, G_0/G_1 同构于 k 的剩余类域 f 的乘法群 f^\times 的一个子群, 而 $G_i/G_{i+1} (i \geq 1)$ 同构于加法群 f^+ 的子群. 从而 G 是可解群.

证明 由于 k'/k 是完全分歧的, 给定 k' 的素元 π' , 由前节末

尾的注记可知 $\sigma' = \sigma[\pi']$, 从而

$$G_i = \{\sigma \in G \mid \sigma(\pi') \equiv \pi' \pmod{p^{i+1}}\}.$$

但是由引理 3 知道 π' 和 $\sigma(\pi')$ 均属于 \mathfrak{p}' , 从而 $G = G_0$. 另一方面, 由 $k' = k(\pi')$ 可知当 $\sigma \neq 1$ 时 $\sigma(\pi') \neq \pi'$, 因此在 $i \geq v'(\sigma(\pi') - \pi')$ 时 $\sigma \notin G_i$. 于是当 i 充分大时 $G_i = 1$. 又由上述的注记可知对于 G_0 中每个元素 σ , \mathfrak{o} 中存在元素 x 使得 $\sigma(\pi') \equiv x\pi' \pmod{p^2}$, 于是 $x \in \mathfrak{p}$. 同样地, 对于元素 $\sigma \in G_i (i \geq 1)$, \mathfrak{o} 中存在元素 y 满足 $\sigma(\pi') \equiv \pi' + y\pi'^{i+1} \pmod{p^{i+2}}$. 不难验证, 映射

$$G_0/G_1 \rightarrow \mathfrak{f}^\times, \sigma \mapsto x \pmod{\mathfrak{p}},$$

$$G_i/G_{i+1} \rightarrow \mathfrak{f}^+, \sigma \mapsto y \pmod{\mathfrak{p}}$$

均是单同态. 由此 $G_i/G_{i+1} (i \geq 0)$ 均是 Abel 群, 又当 i 充分大时 $G_i = 1$, 从而 G 是可解群.

注记 一般地, 如果 k'/k 不一定是完全分歧, 令 $\text{Aut}(\mathfrak{f}/\mathfrak{f})$ 表示剩余类域 \mathfrak{f} 的 \mathfrak{f} -自同构群, 可以证明

$$G/G_0 \cong \text{Aut}(\mathfrak{f}/\mathfrak{f}).$$

并且 G_0 是可解群.

现在讨论更特殊的情形. 设 p 是任意素数, k'/k 为 p 次完全分歧循环扩张. 这时 $G = \text{Gal}(k'/k)$ 是 p 阶循环群, 根据上述定理, 存在适当的整数 $s \geq 1$, 使得

$$G = G_0 = \cdots = G_{s-1}, G_s = 1.$$

令 $\sigma \in G$, $\sigma \neq 1$, 则 $\sigma \in G_{s-1}$, 而 $\sigma \notin G_s$, 由上述定理的证明和 G_s 的定义可知

$$v'(\pi' - \sigma(\pi')) = s.$$

象 §1.1 中那样定义 $U_i = 1 + \mathfrak{p}^i$ 而令 U' 为 k' 的单位群, 则下面的定理在今后是极为重要的.

定理 5 设 $N_{k'/k}$ 是 k' 对于 k 的范, 则

$$U_s \subseteq N_{k'/k}(U').$$

证明 设 π' 为 k' 的素元, 由于 k'/k 是完全分歧的, $k = k(\pi')$, 从而 π' 是 $k[X]$ 中不可约多项式

$$f(X) = X^p + c_1 X^{p-1} + \cdots + c_p, \quad c_i \in k$$

的根, c_i 为 $\{\sigma(\pi') | \sigma \in G\}$ 的对称多项式. 由于 $\sigma(\pi') \in \mathfrak{p}'$, 从而 $v(c_i) \geq 1$ (参考引理 4 后面的注记). 此外, 由于 $f(k'/k) = 1$, 从而由定理 3 的系可知 $v(c_p) = v(\pm N_{k'/k}(\pi')) = v'(\pi') = 1$. 于是 $f(X)$ 是 Eisenstein 多项式. 特别地, 对于 U_s 中任意元素 u , $v(uc_p) = v(c_p) = 1$, 从而

$$g(X) = X^p + c_1 X^{p-1} + \cdots + c_{p-1} X + uc_p$$

也是 Eisenstein 多项式, 因此它在 $k[X]$ 中不可约. 设 F 是将 $g(X)$ 的一个根 α 添加到 k' 中而得到的域, 又令 $k'' = k(\alpha)$, 则

$$F = k'(\alpha) = k'k'', \quad k'' = k(\alpha), \quad g(\alpha) = 0.$$

假如 $k' \neq k''$, 则由于 $p = [k':k]$ 是素数, 从而 $k' \cap k'' = k$. 因此 F/k'' 为 p 次循环扩张, 并且 $\text{Gal}(F/k'') = \text{Gal}(k'/k) = G$. 设 \tilde{v} 是完备域 F 的正规赋值, 则由 §1.2 的引理 3 可知, 对于任意的 $\sigma \in G$ 均有

$$\tilde{v}(\alpha - \sigma(\pi')) = \tilde{v}(\sigma(\alpha - \pi')) = \tilde{v}(\alpha - \pi').$$

从而令 $e = e(F/k')$, $\tilde{v}|_{k'} = ev'$, 则

$$ev'(\pi' - \sigma(\pi')) = \tilde{v}(\pi' - \alpha + \alpha - \sigma(\pi')) \geq \tilde{v}(\alpha - \pi').$$

如果 $\sigma \neq 1$, 则由于 $v'(\pi' - \sigma(\pi')) = s$, 从而得到

$$\tilde{v}(\alpha - \pi') \leq es.$$

因此对于

$$f(X) = \prod_{\sigma \in G} (X - \sigma(\pi')),$$

有

$$\tilde{v}(f(\alpha)) = \sum_{\sigma \in G} \tilde{v}(\alpha - \sigma(\pi')) = p\tilde{v}(\alpha - \pi') \leq pes.$$

另一方面, 由于 k'/k 完全分歧, 从而 $e(k'/k) = p$, $\tilde{v}|_k = ev'|_k = epv$. 此外由 $v(c_p) = 1$ 和 $u \in U_s = 1 + \mathfrak{p}'$ 可知

$$\begin{aligned} \tilde{v}(f(\alpha)) &= \tilde{v}(f(\alpha) - g(\alpha)) = \tilde{v}(c_p - uc_p) \\ &= epv(c_p(1 - u)) \geq ep(1 + s). \end{aligned}$$

而这与前面的不等式相矛盾. 从而证明了 $k' = k''$, $F = k'$ 于是 $\alpha \in k'$. 由于 $g(X)$ 为 $k[X]$ 中不可约多项式, $g(\alpha) = 0$ 并且

$N_{k'/k}(\alpha) = (-1)^r u c_p$, 再由定理 3 的系 3.1 和 $v'(\alpha) = v(u c_p)$
 1. 但是 $N_{k'/k}(\pi) = (-1)^r c_p$, $v'(\pi) = 1$, 所以令 $\xi = \alpha/\pi$, 则

$$u = N_{k'/k}(\xi), \xi \in U'.$$

这就证明了定理.

第二章 闭完备域

本章中考查剩余类域是代数封闭域的完备域。由于没有见到过适当的术语，在本书中我们将这种域叫作闭完备域。例如当 F 是任意的代数封闭域时，§1.3 中例 2 的幂级数域 $F((X))$ 便是闭完备域。Serre^[12] 最先对闭完备域作了实质性的研究。我们要证明在今后要用到的某些结果。

§2.1 范映射

设 K 是对于完备正规赋值 v_K 的闭完备域， $\mathfrak{o}_K, \mathfrak{p}_K$ 分别是 K 的赋值环和极大理想。按照定义，剩余类域 $\mathfrak{k}_K = \mathfrak{o}_K/\mathfrak{p}_K$ 是代数封闭域。

引理 1 K 的任意有限扩域 L 也是闭完备域，并且 L/K 是完全分歧扩张。特别地，若 L/K 是 Galois 扩张，则 $\text{Gal}(L/K)$ 是可解群。

证明 根据 §1.3 定理 2 即知 L 是对于 v_L 的完备域，其中 v_L 是 L 中满足 $v_L|_K \sim v_K$ 的唯一的正规赋值。 L 的剩余类域为 $\mathfrak{k}_L = \mathfrak{o}_L/\mathfrak{p}_L$ 。设 $e = e(L/K)$ ， $f = f(L/K)$ ，由 §1.3 定理 3 可知 $ef = n = [L:K]$ 。由定义可知 $f = [\mathfrak{k}_L:\mathfrak{k}_K]$ ，但是 \mathfrak{k}_K 为代数封闭域而 f 有限，从而 $\mathfrak{k}_L = \mathfrak{k}_K$ ，即 $f = 1$ 。于是 $e = n$ ，即 L 是闭完备域并且 L/K 是完全分歧扩张。如果 L/K 是 Galois 扩张，则由 §1.4 定理 4 可知 $\text{Gal}(L/K)$ 是可解群。

特别对于上述的 L/K ，若将 L 对于 K 的范 $N_{L/K}$ 简单地表示为 N ，则范映射给出乘法群同态

$$N = N_{L/K}: L^\times \rightarrow K^\times.$$

若将 K 的单位群 U_K 也简记成 U ，根据 §1.1 它的子群 $U \cdot (i \geq 0)$ 定

义为

$$U_0 = U = U_K, U_i = 1 + \mathfrak{p}_K^i \ (i \geq 1).$$

同样地, 将 L 的单位群记成 $U_L = U'_0$, 而令 $U'_i = 1 + \mathfrak{p}_L^i \ (i \geq 1)$. 由 §1.3 定理 3 中的系之公式, 可知 $N: L^\times \rightarrow K^\times$ 将 $U' = U_L$ 映到 $U = U_K$ 之中:

$$N(U') \subseteq U.$$

另一方面, 如果令 π' 为 L 中素元, 从 $f = f(L/K) = 1$ 可知 $\pi = N(\pi')$ 是 K 中素元, 从而有 (§1.1)

$$L^\times = \langle \pi' \rangle \times U', \quad K^\times = \langle \pi \rangle \times U.$$

所以下面两个等式是等价的:

$$N(L^\times) = K^\times, \quad N(U') = U.$$

事实上, 这两个等式是成立的. 现在分成几步来证明这一点.

引理 2 如果 L/K 是素次数循环扩张, 则 $N(U') = U$.

证明 令 $[L:K] = p$, $G = \text{Gal}(L/K)$. 正如 §1.4 定理 5 所述, 在这种情形下存在着适当的整数 $s \geq 1$, 使得

$$G = G_s = \dots = G_{s-1}, \quad G_s = 1.$$

并且对于 $\sigma \in G$, $\sigma \neq 1$, 我们有

$$v_L(\pi' - \sigma(\pi')) = s. \quad (1)$$

由同一定理还知道 $U_i \subseteq N(U')$. 因此, 为了证明引理, 只需证明对于每个 i , $0 \leq i < s$, U_i/U_{i+1} 的每个剩余类中均包含 $N(U')$ 中元素即可, 先考虑 $i = 0$ 的情形. 设 u 为 $U = U_0$ 中任意元素, 由于 $k_K = \mathfrak{o}_K/\mathfrak{p}_K$ 是代数封闭域, 所以存在元素 $x \in \mathfrak{o}_K$ 使得 $x^p = u \bmod \mathfrak{p}_K$. 由于 $x \in U$, 从而 $x \in U'$. 因为 $N(x) = x^p$, 这就表明 U_0/U_1 的每个剩余类均包含 $N(U')$ 中的元素. (以上证明并不需要假定 L/K 是素次数循环扩张.)

以下设 $i \geq 1$. 于是可假定 $s \geq 2$. 首先考虑 $p \nmid i$ 的情形 (例如 $i = 1$ 时即是如此). 假设 $\alpha = \pi'^i$, 由 §1.2 中引理 3 可知, 对于任意的 $\sigma \in G$, $\sigma \neq 1$, 我们有 $v_L(\sigma(\pi')) = v_L(\pi') = 1$, 于是由 (1) 式便有

$$v_L(\alpha - \sigma(\alpha)) = v_L(\pi' - \sigma(\pi')) + v_L(\pi'^{i-1} + \dots + \sigma(\pi')^{i-1})$$

$$\geq s + i - 1.$$

其次令

$$f(X) = \prod_{\sigma \in G} (X - \sigma(\alpha)) = X^p + a_1 X^{p-1} + \cdots + a_p, \quad a_i \in K,$$

将多项式 $f(X)$ 求微商然后令 $X = \alpha$, 则得到

$$\prod_{\sigma \neq 1} (\alpha - \sigma(\alpha)) = p\alpha^{p-1} + (p-1)a_1\alpha^{p-2} + \cdots + a_{p-1}.$$

然后由上面关于 $v_L(\alpha - \sigma(\alpha))$ 的不等式, 即得到

$$v_L\left(\sum_{i=0}^{p-1} (p-i)a_i\alpha^{p-i-1}\right) \geq (p-1)(s+i-1), \text{ 而 } a_0 = 1.$$

由于 $e(L/K) = p$, $v_L K = pv_K$, $(p-i)a_i \in K$, 从而当 $(p-i)a_i \neq 0$ 的时候, 我们有

$$v_L((p-i)a_i\alpha^{p-i-1}) \equiv (p-i-1)i \pmod{p}, \quad 0 \leq i \leq p-1.$$

由假定 $p \nmid i$, 因此由上面的同余式可知 $v_L((p-i)a_i\alpha^{p-i-1})$ ($0 \leq i < p-1$) 均不为 $+\infty$ 并且是彼此相异的整数. 从而 $v_L\left(\sum_{i=0}^{p-1} (p-i)a_i\alpha^{p-i-1}\right)$ 等于 $v_L((p-i)a_i\alpha^{p-i-1})$ ($0 \leq i \leq p-1$)

中的最小值. 从而对于每个 $0 \leq i \leq p-1$ 均有 $v_L((p-i)a_i\alpha^{p-i-1}) \geq (p-1)(s+i-1)$, 即

$$\begin{aligned} v_L((p-i)a_i) &\geq (p-1)(s+i-1) - (p-i-1)i \\ &= (p-1)(s-1) + i. \end{aligned}$$

特别取 $i = 0$, 由于 $a_0 = 1$ 是 K 中单位元素, 从而当 $s \geq 2$ 时便有

$$v_L(p \cdot 1) \geq (p-1)(s-1) > 0. \quad (2)$$

于是当 $1 \leq i \leq p-1$ 时 $v_L((p-i) \cdot 1) = 0$. 从而

$$\begin{aligned} v_L(a_i) &= v_L((p-i)a_i) \geq (p-1)(s-1) + i \geq (p-1)i \\ &\quad + i - pi, \end{aligned}$$

即得到

$$v_K(a_i) \geq i \quad (1 \leq i \leq p-1).$$

另一方面, 由于 $v_K(a_i) = v_K(1 + N(\pi')) = v_L(\pi') = i$, 从而

$$a_i = b_i \pi' \quad (1 \leq i \leq p),$$

其中 $b_i \in \mathfrak{o}_K$. 特别地, $b_p \in U - U_K$. 再利用 $\mathfrak{k}_K = \mathfrak{o}_K / \mathfrak{p}_K$ 是代数封闭域, 可知对于每个元素 $a \in \mathfrak{o}_K$, 均存在 $x \in \mathfrak{o}_K$ 使得

$$b_1 x + b_2 x^2 + \cdots + b_p x^p = a \pmod{\mathfrak{p}_K}.$$

对于这个 x 则有

$$N(1 - x\alpha) = 1 + a_1 x + \cdots + a_p x^p$$

$$1 + (b_1 x + \cdots + b_p x^p) \pi' = 1 + a \pi' \pmod{\mathfrak{p}_K^{i+1}}.$$

于是 $1 - x\alpha$ 必然属于 $U' = U_L$. 此外, 由于 U' 是由 $1 + a\pi'$ ($a \in \mathfrak{o}_K$) 形成的, 从而 U_i / U_{i+1} 的每个剩余类均包含 $N(U')$ 中的元素.

最后, 对于 $i \geq 1, s \geq 2, p \nmid i$ 的情形, 令 $i = pi', \alpha = \pi'$, 而

$$\begin{aligned} f(X) &= \prod_{\sigma \in G} (X - \sigma(\alpha)) = (X - \alpha)^p \\ &= X^p + a_1 X^{p-1} + \cdots + a_p, a_i = (-1)^i \binom{p}{i} \alpha^i. \end{aligned}$$

当 $1 \leq i \leq p-1$ 时, 由于 $\binom{p}{i}$ 均可以被 p 整除, 从而由 (2) 式 ((2) 式对于 $i=1$ 的情形已证明是对的)

$$v_L(a_i) \geq (p-1)(s-1) + pi' \geq (p-1)i + i = pi.$$

于是又得到

$$v_K(a_i) \geq i \quad (1 \leq i \leq p-1).$$

由于 $v_K(a_p) = v_K(\alpha^p) = v_K(\pi') = 1$, 然后便与上面同样地证明出 U_i / U_{i+1} 的每个剩余类均包含 $N(U')$ 中元素. 于是证明了引理.

引理 3 假设 K 的特征为 $p > 0$, L/K 为 p 次纯不可分扩张, 则 $N(U') = U$.

证明 在这种情形下, 对于 L 中任意元素 α 均有 $N(\alpha) = \alpha^p$, 又由引理 1 知 L/K 是完全分枝的, 从而若 π' 是 L 中素元, 则 $\pi = N(\pi') = \pi'^p$ 为 K 中素元. 对于 $U_i = 1 + \mathfrak{p}_K^i$ ($i \geq 1$) 中任意元素 $u = 1 + a\pi'$ ($a \in \mathfrak{o}_K$), 由于 $\mathfrak{k}_K = \mathfrak{o}_K / \mathfrak{p}_K$ 是代数封闭域, 从而存在元素 $x \in \mathfrak{o}_K$ 使得 $x^p = a \pmod{\mathfrak{p}_K}$. 令 $\alpha = 1 + x\pi'$, 则 $\alpha \in U_i = 1 + \mathfrak{p}_K^i$. 于是

$$N(\alpha) = \alpha^p - 1 + x^p \pi^{i/p} \equiv 1 + a\pi^i = u \pmod{p_K^{i+1}}.$$

从而 U_i/U_{i+1} 的每个剩余类均包含 $N(U')$ 中的元素, 当 $i = 0$ 时这也是成立的, 因为这已在前一引理证明一开始时就作了说明. 所以对于 $U = U_0$ 中任意元素 u , 均可依次决定出 U' 中元素 $\alpha_0, \alpha_1, \alpha_2, \dots$, 使得对于每个 $i \geq 0$ 均有

$$\alpha_i \in U \quad 1 + p_L^i, \quad N(\alpha_0 \alpha_1 \cdots \alpha_i) = u \pmod{p_K^{i+1}}.$$

由于 L 对于 v_L 是完备的, 可知无限乘积

$$\alpha = \prod_{i=0}^{\infty} \alpha_i$$

在 L 中收敛, 显然

$$\alpha \in U', \quad N(\alpha) = u.$$

因此 $N(U') = U$.

有了以上的准备工作, 现在可以证明闭完备域理论中以下的基本定理.

定理 1 设 L 为闭完备域 K 的任意有限扩域, 则

$$N(L^\times) = K^\times, \quad N(U_L) = U_K.$$

证明 我们已经说过, 只需证明第二个等式即可. 由于 L/K 是有限扩张, 从而可以选取适当的多项式 $f(X) \in K[X]$, 使得 L 包含在 M 之中, 其中 M 是 $f(X)$ 在 K 上的分裂域 $K \subseteq L \subseteq M$. 设 M' 是 M 中 K 的最大可分扩域, 则 M'/K 是 Galois 扩张, 由引理 1 可知 $\text{Gal}(M'/K)$ 是可解群, 从而 M'/K 存在中间域序列: $K = M_0 \subset M_1 \subset \cdots \subset M_n = M'$, 使得 $M_i/M_{i-1} (1 \leq i \leq n)$ 均是素次数的循环扩张. 由引理 2 可知 $N(U_{M_i}) = U_{M_{i-1}} (1 \leq i \leq n)$, 从而 $N(U_{M'}) = U_K$. (其中前一个 N 是 M_i 对于 M_{i-1} 的范, 而后一个 N 是 M' 对于 K 的范.) 另一方面, M/M' 是纯不可分扩张, 如果 $M \neq M'$, 则 M' 的特征 $p > 0$, 并且存在中间域序列: $M' = M'_0 \subset M'_1 \subset \cdots \subset M'_m = M$, 使得 $[M'_i : M'_{i-1}] = p (1 \leq i \leq m)$. 利用引理 3 可以象上面一样地证明 $N(U_M) = U_{M'}$, 再由于 $N(U_{M'}) = U_K$ 即得到 $N(U_M) = U_K$. 由于 $K \subseteq L \subseteq M$, 不难看出有 $N(U_L) =$

U_K .

Serre 在 [11] 第三章 §3 中详细地研究了任意完备域的范映射. 对于它的特殊情形, 即对于闭完备域证明了上面的定理 1. 他在证明中用到关于完备域共轭差积的结果, 我的证明避而不用这个, 而代之以第一章 §1.4 的定理 5, 因此可以说这是定理 1 的一个简单证明.

§ 2.2 基本正合序列

我们继续假设 K 是任意的闭完备域, L 是 K 的任意有限扩域, $v_K, v_L, f_K = f_L$ 等如前节所述, 本节考查 L/K 是 Galois 扩张的情形. 令

$$G = \text{Gal}(L/K),$$

根据 §1.2 的引理 3, 对于 L^\times 中任意元素 α 和 G 中任意元素 σ , $\alpha^{\sigma^{-1}} = \sigma(\alpha)/\alpha$ 包含在 L 的单位群 U_L 之中. 形如

$$\xi^{\sigma^{-1}} = \sigma(\xi)/\xi, \quad \xi \in U_L, \quad \sigma \in G$$

的全部元素 $\xi^{\sigma^{-1}}$ 生成 U_L 的一个子群, 表示成 $V_{L/K}$. 其次, 固定 L 中一个素元 π' , 然后对于 G 的任意元素 σ , 将 $\pi'^{\sigma^{-1}} = \sigma(\pi')/\pi'$ 在 $U_L/V_{L/K}$ 中的剩余类记成 $i(\sigma)$, 即

$$i(\sigma) = \sigma(\pi')/\pi' \pmod{V_{L/K}}.$$

引理 4 $i(\sigma)$ 只依赖于 σ 而与 L 中素元 π' 的取法无关. 并且 $\sigma \mapsto i(\sigma)$ 定义出同态

$$i: G \rightarrow U_L/V_{L/K}.$$

证明 假设 π'_1 是 L 中另一素元, 则 $\pi'_1 = \pi'\xi$, 其中 $\xi \in U_L$. 从而

$$\sigma(\pi'_1)/\pi'_1 = (\sigma(\pi')/\pi')(\sigma(\xi)/\xi) \equiv \sigma(\pi')/\pi' \pmod{V_{L/K}}.$$

即 $i(\sigma)$ 与 π' 的取法无关. 对于 $\tau \in G$, $\tau(\pi')$ 也是 L 的素元, 因而

$$(\sigma\tau)(\pi') = (\sigma(\tau(\pi'))/\tau(\pi'))(\tau(\pi')/\pi'),$$

由此得出 $i(\sigma\tau) = i(\sigma)i(\tau)$.

由于 $U_L/V_{L/K}$ 是 Abel 群, 因此若令 $G' = [G, G]$ 是 G 的换

位子群,而

$$G^{ab} = G/G',$$

则上述的 $i: G \rightarrow U_L/V_{L/K}$ 诱导出同态

$$G^{ab} \rightarrow U_L/V_{L/K}.$$

为简单起见,这个诱导出来的同态仍记为 i . 如果象以前一样将 L/K 的范映射记为 $N = N_{L/K}$, 则对于 L^* 中任意元素 α 显然有 $N(\sigma(\alpha)/\alpha) = 1$. 特别地 $N(V_{L/K}) = 1$. 从而范映射定义出同态

$$N = N_{L/K}: U_L/V_{L/K} \rightarrow U_K.$$

于是得到 Abe. 群同态序列

$$1 \rightarrow G^{ab} \xrightarrow{i} U_L/V_{L/K} \xrightarrow{N} U_K \rightarrow 1. \quad (3)$$

现在我们分成几步证明这是正合序列. 由上节定理 1 知道 $N: U_L/V_{L/K} \rightarrow U_K$ 是满射. 其次注意到显然有 $\text{Im}(i) \subseteq \text{Ker}(N)$. 从而只需证明 $G^{ab} \xrightarrow{i} U_L/V_{L/K}$ 是单射以及 $\text{Ker}(N) \subseteq \text{Im}(i)$.

引理 5 如果 L/K 是循环扩张, 则(3)是正合序列.

证明 设 $[L:K] = n$, 则 $G = \text{Gal}(L/K)$ 是 n 阶循环群, 于是 $G = G^{ab}$. 设 ρ 是 G 的生成元, 不难看出

$$V_{L/K} = U_L^{G^{ab}} = \{\xi^{\rho^{-1}} = \rho(\xi)/\xi \mid \xi \in U_L\}.$$

因此若 $\sigma = \rho^s \in \text{Ker}(i)$, 则 $i(\sigma) = i(\rho)^s = 1$, 从而存在 $\xi \in U_L$ 使得

$$(\rho(\pi')/\pi')^s = \rho(\xi)/\xi.$$

因此 $x = \pi'^s/\xi \in K$, 根据引理 1, L/K 是完全分歧的, 从而 $v_L|K = nv_K$, 于是

$$s = v_L(\pi'^s/\xi) = nv_K(x) \equiv 0 \pmod{n}.$$

从而 $\sigma = \rho^s = 1$. 于是证明了 $\text{Ker}(i) = 1$. 其次, 假设 $\eta \in U_L$, $N(\eta) = 1$, 则由熟知的 Hilbert 定理可知存在元素 $\alpha \in L^*$ 使得

$$\eta = \alpha^{\rho^{-1}}.$$

令 $\sigma = v_L(\alpha)$, 则 $\alpha = \pi'^s \xi$, $\xi \in U_L$. 于是

$$\eta = (\rho(\pi')/\pi')^s (\rho(\xi)/\xi) \equiv \rho^s(\pi')/\pi' \pmod{V_{L/K}}.$$

从而证明了 $\text{Ker}(N) \subseteq \text{Im}(i)$.

现在仍设 L/K 是一般的 Galois 扩张, 设 M 是 L/K 的中间域: $K \subseteq M \subseteq L$, 并且 M/K 亦是 Galois 扩张. $\text{Gal}(L/K)$ 中任意元素 σ 在子域 M 上的限制给出 $\text{Gal}(M/K)$ 中元素 $\sigma' = \sigma|_M, \sigma \mapsto \sigma' = \sigma|_M$ 定义出满同态

$$\text{Gal}(L/K) \rightarrow \text{Gal}(M/K).$$

另一方面, 对于任意元素 $\alpha \in L^\times$, 显然有

$$N_{L/M}(\alpha^{\sigma^{-1}}) = N_{L/M}(\sigma(\alpha)/\alpha) = \sigma'(N_{L/M}(\alpha))/N_{L/M}(\alpha) = N_{L/M}(\alpha)^{\sigma'-1},$$

根据定理 1 有 $N_{L/M}(U_L) = U_M$, 从而由上式得到

$$N_{L/M}(V_{L/K}) = V_{M/K}. \quad (4)$$

从而范映射 $N_{L/M}$ 诱导出同态

$$U_L/V_{L/K} \rightarrow U_M/V_{M/K}.$$

将它与上述 Galois 群之间的同态合在一起, 就得到图表

$$\begin{array}{ccccc} \text{Gal}(L/K) & \xrightarrow{i} & U_L/V_{L/K} & \xrightarrow{N} & U_K \\ \downarrow & & \downarrow & & \parallel \\ \text{Gal}(M/K) & \xrightarrow{i} & U_M/V_{M/K} & \xrightarrow{N} & U_K \end{array} \quad (5)$$

由于 $N_{L/M}(\pi')$ 是 M 的素元并且 $N_{L/K} = N_{M/K} \circ N_{L/M}$, 立刻知道图表 (5) 是交换的.

引理 6 $i: G^{ab} \rightarrow U_L/V_{L/K}$ 是单射.

证明 设 $\sigma \in G = \text{Gal}(L/K)$ 并且 σ 不属于 G 的换位子群 G' , 由于 $G^{ab} = G/G'$ 是 Abel 群, 从而存在 G 的一个正规子群 H , 使得

$$G' \subseteq H \subseteq G, \quad G/H \text{ 是循环群, } \sigma \notin H.$$

令 M 是对应于 H 的 L/K 之中间域, 则 M/K 是 Galois 扩张并且 $\text{Gal}(M/K) = G/H$. 如上令 $\sigma' = \sigma|_M$, 由于 $\sigma \notin H$, 从而 $\sigma' \neq 1$. 但是由前一引理知 $i: \text{Gal}(M/K) \rightarrow U_M/V_{M/K}$ 是单射, 从而 $i(\sigma') \neq 1$. 再由交换图表 (5) 即知 $i(\sigma) \neq 1$. 从而 $i: G^{ab} \rightarrow U_L/V_{L/K}$ 是单射.

定理 2 对于任意有限 Galois 扩张, 我们有正合序列

$$1 \rightarrow \text{Gal}(L/K)^{ab} \xrightarrow{i} U_L/V_{L/K} \xrightarrow{N} U_K \rightarrow 1.$$

证明 从开始时的注记和上面的引理 6 可知只需证明

$\text{Ker}(N) \subseteq \text{Im}(i)$ 即可. 现在对于 $n = [L:K]$ 作数学归纳法. $n = 1$ 的情形显然成立. 设 $n > 1$, 由引理 1 知道 L/K 是可解扩张, 从而存在中间域 M 使得

$$K \subset M \subset L, K \neq M, M/K \text{ 为循环扩张.}$$

象前由引理 1 取 L 的素元 π' , 则 $N_{L/M}(\pi')$ 为 M 的素元. 如果对于 $\xi \in U_L$, $N_{L/K}(\xi) = 1$, 令 $\xi' = N_{L/M}(\xi)$, 则 $\xi' \in U_M$ 并且 $N_{M/K}(\xi') = 1$. 根据引理 5 可知图表 (5) 下行是正合的, 因此存在 $\sigma' \in \text{Gal}(M/K)$ 使得

$$\sigma'(N_{L/M}(\pi')), N_{L/M}(\pi') \equiv \xi' \pmod{V_{M/K}}.$$

由于 $\text{Gal}(L/K) \rightarrow \text{Gal}(M/K)$ 是满同态, 令 $\sigma \mapsto \sigma'$, 则上面的同余式可以写成

$$N_{L/M}(\sigma(\pi')/\pi') \equiv N_{L/M}(\xi) \pmod{V_{M/K}}.$$

于是由 (4) 式可知 $V_{L/K}$ 中存在适当的元素 η , 使得 $N_{L/M}(\sigma(\pi')/\pi') = N_{L/M}(\xi\eta)$. 如果令 $\lambda = \xi\eta\pi'/\sigma(\pi')$, 则

$$\lambda \in U_L, N_{L/M}(\lambda) = 1.$$

将归纳假设用于 L/M , 则有正合序列

$$\text{Gal}(L/M)^{ab} \xrightarrow{i} U_L/V_{L/M} \xrightarrow{N} U_M,$$

从而由上式可知存在 $\tau \in \text{Gal}(L/M)$, 使得

$$\tau(\pi')/\pi' \equiv \lambda \pmod{V_{L/M}}.$$

由于 $\text{Gal}(L/M) \subseteq \text{Gal}(L/K) = G$, 又由定义即知 $V_{L/M} \subset V_{L/K}$, 从而由上面同余式得到

$$(\sigma(\pi')/\pi')(\tau(\pi')/\pi') \equiv \xi\eta \equiv \xi \pmod{V_{L/K}}.$$

即 $i(\sigma\tau) = \xi \pmod{V_{L/K}}$. 从而证明了 $\text{Ker}(N) \subseteq \text{Im}(i)$.

上面定理 2 中的正合序列叫作 Galois 扩张 L/K 的基本正合序列. 特别若 L/K 是 Abel 扩张, 则有基本正合序列

$$1 \rightarrow \text{Gal}(L/K) \rightarrow U_L/V_{L/K} \rightarrow U_K \rightarrow 1.$$

Serre[12] 中用 $G = \text{Gal}(L/K)$ 的上同调群证明了定理 2, 方法如下: 由正规赋值 v_L 定义出正合序列

$$1 \rightarrow U_L \rightarrow L^\times \rightarrow \mathbf{Z} \rightarrow 1,$$

第三章 局 部 域

完备域 k 的剩余类域 \bar{k} 是有限域, 则称 k 是局部域. 设 \bar{k} 的特征是素数 p , 则 k 也叫作 p 局部域¹⁾. 局部类域论就是关于局部域的代数扩域特别是 Abel 扩域的理论. 本章介绍关于局部域的基本结果.

§ 3.1 局部域的一般性质

以下设 k 是局部域, v 是 k 的完备正规赋值, q 为 k 的剩余类域 $\bar{k} = \mathfrak{o}/\mathfrak{p}$ 的元素个数. 如果 k 为 p 局部域, 则 q 为 p 的幂. 并且在这种情形下, $p\mathfrak{o} \subset \mathfrak{p}$, $v(p \cdot 1) > 0$, 因此 k 的特征或者是 0 或者是 p . §1.3 中例 1 的 p -adic 域 \mathbb{Q}_p 是特征为 0 的 p 局部域, 另一方面, 在那里的例 2 中取 $F = \mathbb{F}_p$ (p 个元素组成的有限域), 则幂级数域 $\mathbb{F}_p((X))$ 是特征为 p 的 p 局部域.

引理 1 局部域 k 中包含多项式 $X^q - X$ 的 q 个不同的根, 这些根组成的集合 A 形成 $\bar{k} = \mathfrak{o}/\mathfrak{p}$ 在 \mathfrak{o} 中的完全代表系.

证明 由于 \bar{k} 是由 q 个元素形成的有限域, 从而多项式 $X^q - X$ 在 \bar{k} 中恰好具有 q 个不同的根. 根据 §1.2 引理 1 可知 $X^q - X$ 在 \mathfrak{o} 中也有 q 个根, 并且这些根代表 $\bar{k} = \mathfrak{o}/\mathfrak{p}$ 的每个剩余类. 因此集合 A 是 $\bar{k} = \mathfrak{o}/\mathfrak{p}$ 在 \mathfrak{o} 中的完全代表系. 注意 A 包含 k 的零元素 0.

系 以 V 表示 k 中包含的全部 $(q-1)$ 次单位根, 则 V 是 $q-1$ 阶循环群, 并且自然满同态 $\mathfrak{o} \rightarrow \bar{k} = \mathfrak{o}/\mathfrak{p}$ 诱导出乘法群同构

1) 局部域 词各人所用的意义不完全一致. 例如有人也把第一章中定义的完备域叫做局部域. p 局部域是根据 Weil [14] 中的 “ p field” 所给的名字.

$$V \cong F^*$$

证明 引理 1 中的集合 A 去掉 0 之后即为集合 V , 因此显然有同构 $V \cong F^*$. 由于 F^* 是 $q - 1$ 阶循环群, 从而 V 也如此.

一般地, 设 k' 是 k 的任意有限扩域. 根据 §1.3 定理 2, k' 是完备域, 并且具有唯一的正规赋值 v' , 使得 $v'|_k \sim v$. 设 k' 的剩余类域为 $\bar{k}' = o'/p'$, 由 §1.3 定理 3 可知 $[k'/k] = [f':f]$ 有限, 从而 \bar{k}' 与 \bar{k} 一样也是有限域. 因此我们知道, 局部域 k 的有限扩域也必然是局部域. 注意由于 \bar{k} 是有限域, 从而有限扩张 f'/f 是 Galois 扩张, 特别若 k 是 p 局部域, 则 k' 也是 p 局部域, 所以上面所述的 p 局部域 O_p 和 $F_p((X))$ 的有限扩域均是 p 局部域. 其逆命题也成立:

定理 1 每个 p 局部域 (作为局部域) 均同构于 O_p 或者 $F_p((X))$ 的某个有限扩域. 特别地, 若 k 的特征为 p , 则 k 包含一个子域 F 与 k 的剩余类域 \bar{k} 同构, 从而有 F -同构 $k \cong F((X))$.

证明 如果 k 的特征是 0, 则 k 包含有理数域 \mathbb{Q} , 又由 $p \in p$ 知道 $e = v(p) \geq 1$. 限制 $v|_{\mathbb{Q}}$ 与 \mathbb{Q} 上的 p -adic 赋值是等价的¹⁾. 由于 v 是完备的, \mathbb{Q} 在 k 中的闭包 $\bar{\mathbb{Q}}$ 是 \mathbb{Q} 对于赋值 $v|_{\mathbb{Q}}$ 的完备化, 因此 $\bar{\mathbb{Q}} = O_p$. 另一方面, k 的剩余类域 \bar{k} 是特征为 p 的有限域, 从而是 O_p 的剩余类域 F_p 的有限扩张. 令 $f = [f: F_p]$, 由 §1.3 定理 3 的证明可知 $[k: O_p] = ef < +\infty$. 从而 k 是 (同构于) O_p 的有限扩域.

其次设 k 的特征为 p . 引理 1 中的集合

$$A = \{x \in k \mid x^q = x\}$$

显然是 k 的子域. 将它改记为 F , 则 $o \rightarrow \bar{o} = o/p$ 诱导出有限域的同构 $F \cong \bar{k}$. 设 π 是 k 的素元, 由 §1.3 定理 1 立即知道, $X \mapsto \pi$ 定义出 F -同构

$$F((X)) \cong k.$$

由于 F 的特征为 p 而 F/F_p 是有限扩张, 从而 $F((X))$ 也是

1) 证明: 参见 v. d. Waerden [13], 第十章.

$F_p((X))$ 的有限扩张。这就证明了定理。

注记 一般地, 如果 k 是特征为 p 的完备域, 并且 k 的剩余类域 \bar{k} 是完全域¹⁾, 则可以证明同样的结果: $k \simeq F((X))$, $F \simeq \bar{k}$ ²⁾. 此外, 根据上述定理知道 k 是 $F_p((X))$ 的有限扩域, 从而取 F_p 的适当的有限扩域 F , 则必有 $k \simeq F((X))$ (但不一定是 $F_p((X))$ 同构).

现在考查局部域的拓扑性质。

定理 2 局部域 k 是非离散的全不连通的局部紧域. k 的赋值环 \mathfrak{o} 和极大理想的幂 $\mathfrak{p}^n (n \geq 1)$ 均是 k 的紧开加法子群, 并且 \mathfrak{o} 是 k 的最大紧子环.

证明 由于 v 是正规赋值, 在 §1.1 中已经说过 k 是非离散的全不连通拓扑域, 并且 $\mathfrak{p}^n (n \geq 0)$ 是全体开加法子群. 另一方面, 由于 k 的剩余类域 \bar{k} 是有限域, 它在 \mathfrak{o} 中的完全代表系 A 是有限集合, 从而是紧集合. 因此由 §1.3 定理 1 的系可知 \mathfrak{o} 也是紧集合, 所以 k 是局部紧域. 此外, 由于 \mathfrak{o} 是开加法子群, 从而也是闭加法子群, 因此 $\mathfrak{p}^n (n \geq 0)$ 均是紧的. 最后, 设 R 是 k 的紧子环, 则赋值集合 $\{v(x) | x \in R\}$ 有下界. 对于每个 $x \in R$ 和 $n \geq 1$, 则 $x^n \in R$, 从而 $v(x^n) = nv(x)$, 因此 $v(x) \geq 0$, 即 $x \in \mathfrak{o}$, 从而 $R \subset \mathfrak{o}$, 即 \mathfrak{o} 是 k 的最大紧子环.

注记 由于 \mathfrak{o} 是紧的, 不难直接证明, \mathfrak{o} 对于由 v 所定义的距离 ρ (参见 §1.1) 是完全有界的完备距离空间.

定理 3 局部域 k 的乘法群 k^\times 对于诱导拓扑是非离散并且全不连通的局部紧 Abel 群. 并且 k 的单位群 U 和它的子群 $U_n = 1 + \mathfrak{p}^n (n \geq 1)$ (§1.1) 均是 k^\times 的紧开子群, 而 U 是 k^\times 的最大紧子群, 如果以 V 表示 k 中的 $(q-1)$ 阶单位根乘法群 (引理 1, 系), 则

$$U = V \times U_1, [U:U_n] = (q-1)q^{n-1}, n \geq 1,$$

1) 一个域 F 叫做完全域 (perfect), 如果 F 上每个不可约多项式均是可分的, 或者等价地说, 如果 F 的特征为 0 或者 F 的特征 $\neq p$ 并且 $F = F^p$. 参者注

2) 参见 Serre [11], 第二章, §4.

证明 如在 §1.1 中所述, 自然满同态 $\phi \rightarrow \phi = \phi/p$ 诱导出同构 $U/U_1 \cong \mathbb{F}^*$. 另一方面, 由引理 1 的系知道由 $V \cong \mathbb{F}^*$ 得到 $U \cong V \times U_1$. 又由 §1.1 知道 $U_n/U_{n+1} \cong \mathbb{F}^*(n \geq 1)$, 从而 $[U:U_n] = (q-1)q^{n-1}$. 从定理 2 即知 $U_n = 1 + \mathfrak{p}^n (n \geq 1)$ 是 k^\times 的紧开子群. 由于 $[U:U_1] = q-1$ 可知 U 同样也是 k^\times 的紧开子群, 并且象证明 \mathfrak{o} 是 k 的最大紧子环一样, 可以证明 U 是 k^\times 的最大紧子群, 最后由以上所述不难看出 k^\times 是非离散并且完全不连通的局部紧群.

由于 U_1 是紧的, $[U_1:U_n] = p^n$ 是 p 的幂, 并且 $U_n (n \geq 1)$ 只有 1 是公共元素, 可知 U_1 是有限 p 群 $U_1/U_n (n \geq 1)$ 的射影极限. 从而 U_1 是所谓的射影 p 群 (pro p group). 同样地, 加法群 \mathfrak{o} 是有限 p 群 $\mathfrak{o}/\mathfrak{p}^n (n \geq 1)$ 的射影极限, 因此也是射影 p 群. 所以若 m 是与 p 互素的自然数, 则 $u \mapsto u^m$ 和 $x \mapsto mx$ 分别定义出 U_1 和 \mathfrak{o} 的自同构. 特别地

$$U_1^m = U_1, \quad m\mathfrak{o} = \mathfrak{o}.$$

引理 2 设 k 是特征为 0 的局部域, $m \geq 1$ 为任意自然数, 则 $k^{\times m}$, U^m 和 U_1^m 均是 k^\times 的开子群, 并且 $k^\times/k^{\times m}$, U/U^m 和 U_1/U_1^m 均是有限群. 如果 k 的特征为 p , 那末对于与 p 互素的自然数 m , 上述结果也是对的.

证明 设 k 是 p 局部域. $k^\times/U \cong \mathbb{Z}$, $U \cong V \times U_1$, 并且 U_1 是 k^\times 的开子群, 因此只要证明 U_1^m 是 U_1 的开子群并且 U_1/U_1^m 是有限群即可. 假设 $m = m'p^e$, $(m', p) = 1$, 由上面的注记可知 $U_1^m = U_1^{m'}$, 因此当 k 的特征为 0 时只需考虑 $m = p^e (e \geq 1)$ 的情形即可, 在这种情形下, p 作为 k 中的元素不是 0. 但是剩余类域 $\mathbb{F} = \mathfrak{o}/\mathfrak{p}$ 的特征为 p , 从而 $1 \leq e \leq v(p) < +\infty$. 取 π 为 k 的素元, 考虑 $U_n = 1 + \mathfrak{p}^n = 1 + \mathfrak{o}\pi^n (n \geq 1)$ 中元素 $1 + x\pi^n (x \in \mathfrak{o})$ 的 p 次幂. 由于 $n + e < np$, 并且二项式系数 $\binom{p}{i} (1 \leq i \leq p-1)$ 均可以被 p 除尽, 因此

$$(1 + x\pi^n)^p \equiv 1 + px\pi^n \pmod{\mathfrak{p}^{n+e+1}}.$$

由于 $v(px\pi^n) = n + e$, 由上式可知 U_{n+e}/U_{n+e-1} 的每个剩余类均包

含有 U_1^p 中的元素, 令

$$a = 1 + \left\lfloor \frac{cp}{p-1} \right\rfloor,$$

则每个整数 $b \geq a$ 均可以表示成

$$b = n + c, \quad n + c < np, \quad n \geq 1.$$

利用证明 §2.1 引理 3 的同样方法(或者利用 $U_n, n \geq 1$ 的紧性)得

■

$$U_1 \subset U_1^p \subset U_1.$$

但是 $[U_1: U_1^p] = q^{p-1}$, 从而 U_1/U_1^p 为有限群. 此外, U_1 中的自同态 $x \mapsto x^{p^i}$ 诱导出满同态 $U_1/U_1^p \rightarrow U_1^p/U_1^{p^{i+1}}$. 从而 $U_1^{p^i}/U_1^{p^{i+1}}$ ($i \geq 0$) 也都是有限群. 因此 $U_1/U_1^{p^i}$ 也是有限群. 由于 U_1 是紧的, 从而 $U_1^{p^i}$ 也是紧的, 从而是 U_1 的闭子群. 另一方面, 由于 $[U_1: U_1^{p^i}]$ 有限, 从而 $U_1^{p^i}$ 也是 U_1 的开子群. 于是证明了引理.

今后使用此引理时, 只用上述结果, 即只涉及到 k 的特征为 0 的场合. 注意在这种情况下 $\{U_1^{p^n}\}_{n \geq 1}$ 形成 k^\times 中单位元素 1 的基本邻域系.

注记 如果 k 的特征是 p , 则由定理 1 不难看出 U_1/U_1^p 实际上是无限群.

上面的定理 2 表明, 局部域是非离散并且全不连通的局部紧域. 反过来可以证明, 非离散并且全不连通的局部紧域必然是局部域. 这一结果以后不用到, 但是为参考起见, 下面简单说明一下证明的概要¹⁾, 设 k 是任意非离散的局部紧域, 则 k 的加法群 k^+ 是局部紧 Abel 群, 因此在 k^+ 上存在 Haar 测度 μ . 对于固定的元素 $0 \neq x \in k$, $y \mapsto xy (y \in k^+)$ 是 k^+ 的拓扑自同构, 从而对于 k^+ 的每个 Borel 子集合 S , 由

$$\mu'(S) = \mu(xS)$$

定义的 μ' 也是 k^+ 上的 Haar 测度. 由 Haar 测度的唯一性可知存在常数 $c > 0$, 使得 $\mu' = c\mu$. c 是由 x 所决定的, 因此写成 $c =$

1) 详见 Weil [14], 第 1 章, §4.

$|x|$. 换句话说, 对于 $0 \neq x \in k$ 我们有

$$\mu(xS) = \|x\| \mu(S), \quad S \subseteq k^+.$$

因为 k 是非离散的, k 的每点的测度均是 0. 因此若定义 $0\| = 0$, 则上式对于 k 中每个元素 x 都是对的. 此外, $\|x\|$ 是 x 的连续函数, 并且对于每个实数 $\alpha > 0$, 可以证明 $\{x \in k \mid \|x\| \leq \alpha\}$ 是 k 的紧子集. 由此即知 $\|x\|$ 是 k 上的完备的“绝对值”. 如果绝对值 $\|x\|$ 是阿基米德的, 则 k 同构于实数域 \mathbf{R} 或者复数域 \mathbf{C} , 从而 k 是连通的. 如果 $\|x\|$ 是非阿基米德的, 令 $v(x) = -\log \|x\|$, 则 v 是 k 的赋值, 并且可以证明 v 等价于 k 上的完备正赋估值 v . 由于 (k, v) 是完备域, 而 v 的赋值环 $\mathfrak{o} = \{x \in k \mid v(x) \geq 0\} = \{x \in k \mid \|x\| \leq 1\}$ 是紧的, 从而剩余类域 $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ 是有限域, 从而 k 是局部域. 这就证明了非离散不连通局部紧域必然是局部域.

§ 3.2 有限扩域

上节已经说过, 局部域 k 的有限扩域 k' 仍然是局部域, 现在考查 k'/k 是不分岐扩张的情形.

定理 4 对于每个自然数 $n \geq 1$, k 均存在 (不计 k -同构) 唯一的 n 次不分岐扩域 k' . k' 即是多项式 $X^n - X$ 在 k 上的分裂域, 从而 k'/k 是 n 次循环扩张. 如果 \mathfrak{f} 是 k' 的剩余类域, 则 $\text{Gal}(k'/k)$ 中每个元素 σ 诱导出 $\mathfrak{f}/\mathfrak{f}$ 的自同构 σ' , 并且 $\sigma \mapsto \sigma'$ 定义出自然同构

$$\text{Gal}(k'/k) \xrightarrow{\sim} \text{Gal}(\mathfrak{f}/\mathfrak{f}).$$

证明 先证明 k' 的存在性. 由于 \mathfrak{f} 是有限域, 因此对于每个 $n \geq 1$, \mathfrak{f} 有唯一的 n 次扩域 \mathfrak{f}^* , 并且 $\mathfrak{f}^*/\mathfrak{f}$ 是可分扩张. 因此 $\mathfrak{f}[X]$ 中包含 n 次不可约多项式 $g(X)$. 取 n 次多项式 $f(X) \in \mathfrak{o}[X]$, 使得 $g(X)$ 等于 $f(X) \bmod \mathfrak{p}$. 令 k' 是将 $f(X)$ 的一个根 α 添加到 k 上而得到的域: $k' = k(\alpha)$, $f(\alpha) = 0$. 显然 $[k':k] \leq n$. 我们可以选取 $g(X)$ 和 $f(X)$ 的最高项系数均为 1, 从而 α 是对于 \mathfrak{o} 的整元素. 由 §1.2 引理 4 使知 $\alpha \in \mathfrak{o}'$. 令 \mathfrak{o} 是 $\mathfrak{f} = \mathfrak{o}'/\mathfrak{p}'$ 中包含 α 的剩余

类, 则 $\omega \in \mathfrak{f}$, $g(\omega) = 0$. 由于 $g(X)$ 是 $[X]$ 中 n 次不可约多项式, 从 §1.3 定理 3 即知

$$r = [f(\omega):f] \leq [f':f] = f(k'/k) \leq [k':k] \leq n.$$

因此 $[k':k] = n = f(k'/k)$, 即 k' 是 k 的 n 次不分歧扩域.

现在设 k' 是 k 上任意 n 次不分歧扩域. 由于 $[f':f] = f(k'/k) = n$, 从而 f 是 q^n 个元素的有限域. 根据引理 1, $A' = \{x' \in k' \mid x'^{q^n} = x'\}$ 是 $f' = \mathfrak{o}'/\mathfrak{p}'$ 在 \mathfrak{o}' 中的完全代表系. 如果令 $k'' = k(A')$, 又令 f'' 是 k' 的剩余类域, 则

$$k \subseteq k'' \subseteq k', \quad f \subseteq f' \subseteq f''.$$

由 $A' \subseteq k'$ 可知 $f' = f$. 因此由 §1.3 定理 3 可知

$$n = [f':f] = [f'':f] = f(k''/k) \leq [k'':k] \leq [k':k] = n.$$

从而 $k' = k'' = k(A')$. 换句话说, k' 是 $X^{q^n} - X$ 在 k 上的分裂域. 这也同时证明了 k' 的唯一性. 由于 $X^{q^n} - X$ 在 k' 内有 q^n 个彼此不同的根, 因此 k'/k 是可分扩张, 从而为 Galois 扩张. 另一方面, 由于 f 是有限域, 从而 f'/f 是 n 次循环扩张, 故由 §1.2 引理 3 可知 $\text{Gal}(k'/k)$ 中每个元素 σ 均诱导出 f'/f 的一个自同构 σ' , 并且 $\sigma \mapsto \sigma'$ 显然定义了一个同态 $\text{Gal}(k'/k) \rightarrow \text{Gal}(f'/f)$. σ 将 $X^{q^n} - X$ 的根集合 A' 映成自身, 并且 A' 是 $f' = \mathfrak{o}'/\mathfrak{p}'$ 的完全代表系, 从而若 $\sigma' = 1$, 则由于 $k' = k(A')$ 可知 $\sigma = 1$. 因此 $\text{Gal}(k'/k) \cong \text{Gal}(f'/f)$ 是单同态. 但是这两个 Galois 群的阶相等: $n = [k':k] = [f':f]$, 从而必然 $\text{Gal}(k'/k) \cong \text{Gal}(f'/f)$. 由于 $\text{Gal}(f'/f)$ 是循环群, 因此 $\text{Gal}(k'/k)$ 也是 n 阶循环群, 即 k'/k 为 n 次循环扩张. 这就完全证明了定理.

由于 f 是 q 个元素的有限域, 所以 Galois 群 $\text{Gal}(f'/f)$ 是由自同构

$$\omega \mapsto \omega^q, \quad \omega \in f'$$

组成的. 根据上面定理, 这个自同构对应于 $\text{Gal}(k'/k)$ 的一个元素 φ , 于是 φ 为 $\text{Gal}(k'/k)$ 的生成元, 并且对于每个 $x' \in \mathfrak{o}'$ 均有

$$\varphi(x) \equiv x'^q \pmod{\mathfrak{p}'},$$

并且 φ 是由此同余关系所刻划的 $\text{Gal}(k'/k)$ 中唯一元素. 我们称

φ 为不分歧扩张 k'/k 的 Frobenius 自同构(或者 Frobenius 置换).

例 设 k 是特征为 p 的局部域. 由定理 1 可知 $k = F((X))$, 其中 k 的子域 F 同构于 k 的剩余类域 f . 由于 F 是 q 元有限域, 从而 F 的 n 次扩张 F' 是多项式 $Y^{q^n} - Y$ 在 F 上的分裂域. 于是由定理 4 可知

$$k' = F'((X))$$

是 k 的 n 次不分歧扩张, 并且 k 的每个有限不分歧扩张均可如此得到. k' 的每个元素 x' 是系数属于 F' 的关于 X 的幂级数, 将幂级数 x' 诸系数 a 均改成 a^q , 即得出 $\varphi(x')$ 的幂级数表达式.

现设 k'/k 为任意的 n 次扩张(不必不分歧), 而令

$$e = e(k'/k), f = f(k'/k).$$

定理 5 k' 包含多项式 $X^{q^f} - X$ 在 k 上的分裂域 k_0 , 并且 k_0 是包含在 k' 中的 k 之最大不分歧扩张, $[k_0:k] = f$. 另一方面, k'/k_0 是完全分歧扩张, $[k':k_0] = e$.

证明 设 f 为 k 的剩余类域, 则 $f \approx [f:f]$, 从而 f 是 q^f 个元素的有限域. 由引理 1 即知 k' 包含 $X^{q^f} - X$ 在 k 上的分裂域 k_0 . 由定理 4 知 k_0/k 是 f 次不分歧扩张. 设 k'' 是 k 的任意不分歧扩张并且 $k'' \subseteq k'$, 令 $f_1 = f(k''/k) = [k'':k]$. 再由定理 4 即知 k'' 是 $X^{q^{f_1}} - X$ 在 k 上的分裂域. 由于 $f(k'/k) = f(k'/k'')f(k''/k)$, 从而 f_1 是 f 的因子, 从而 $X^{q^{f_1}} - X$ 能整除 $X^{q^f} - X$. 因此 $k'' \subseteq k_0$, 即 k_0 是包含在 k' 中的 k 之最大不分歧扩张. 由于 k_0/k 不分歧, 从而 $f(k_0/k) = [k_0:k] = f = f(k'/k)$. 于是 $f(k'/k_0) = 1$, 即 k'/k_0 是完全分歧的. 最后由 §1.3 定理 3 给出 $[k':k_0] = [k':k][k_0:k]^{-1} = ef/f = e$.

定理 5 中的 k_0 叫作扩张 k'/k 的惯性域.

引理 3 如果 k'/k 为 Galois 扩张, 则 $\text{Gal}(k'/k_0)$ 即是 §1.4 中定义的 $G = \text{Gal}(k'/k)$ 的正规子群 G_0 :

$$\text{Gal}(k'/k_0) = G_0, \text{Gal}(k_0/k) = G/G_0.$$

证明 从 §1.2 引理 3 可知, $\text{Gal}(k'/k)$ 中每个元素 σ 诱导 f/f 的一个自同构 σ' , 并且 $\sigma \mapsto \sigma'$ 是同态 $\text{Gal}(k'/k) \rightarrow \text{Gal}(f/f)$.

根据定义, G_0 正是这个同态的核. 另一方面, 令 f_0 为 k_0 的剩余类域, 则由定理 4 得到同样的同构 $\text{Gal}(k_0/k) \cong \text{Gal}(f_0/f)$, 图表

$$\begin{array}{ccc} \text{Gal}(k'/k) & \rightarrow & \text{Gal}(f'/f) \\ \downarrow & & \downarrow \\ \text{Gal}(k_0/k) & \cong & \text{Gal}(f_0/f) \end{array}$$

是可交换的, 其中两个竖向箭头分别是由 $\sigma \mapsto \sigma|_{k_0}$ 和 $\sigma \mapsto \sigma|_{f_0}$ 定义的同态. 由于 $f(k'/k) = f = [k_0:k] = f(k_0/k)$, 从而 $f' = f_0$. 因此 G_0 与 $\text{Gal}(k'/k) \rightarrow \text{Gal}(k_0/k)$ 的核 $\text{Gal}(k'/k_0)$ 一致.

对应于惯性域 k_0 的 $G = \text{Gal}(k'/k)$ 之正规子群 G_0 叫做 Galois 扩张 k'/k 的惯性群.

定理 6 设 k' 为局部域 k 的任意有限 Galois 扩张, 则 $\text{Gal}(k'/k)$ 是可解群, 即 k'/k 必为可解扩张.

证明 由引理 3 和定理 4 知 G/G_0 为循环群. 又由定理 5 可知 k'/k_0 是完全分歧扩张, 从而由 §1.4 定理 4 知道 $G_0 = \text{Gal}(k'/k_0)$ 为可解群. 所以 $G = \text{Gal}(k'/k)$ 是可解群.

§ 3.3 局部域的范群

设 k' 为局部域 k 的有限扩域, 令 $N_{k'/k}$ 是 k' 对于 k 的范, U 和 U' 分别为 k 和 k' 的单位群. 显然 $N_{k'/k}(k'^{\times})$ 是 k^{\times} 的乘法子群, 从 §1.3, 定理 3 系中的公式可知

$$N_{k'/k}(U') = N_{k'/k}(k'^{\times}) \cap U.$$

但是从 §3.1, 定理 3 知道 U' 的紧群, 又由 §1.2, 引理 4 知道范映射是连续的, 从而 $N_{k'/k}(U')$ 是 U 的紧子群. 我们把 $N_{k'/k}(k'^{\times})$ 和 $N_{k'/k}(U')$ 分别叫作 k'/k 的范群和单位范群.

引理 4 如果 k'/k 是不分歧扩张, 则 $N_{k'/k}(U') = U$.

证明 如 §1.1 中所述, 利用 k 的素元 π 定义同构

$$U/U_n \cong \mathbb{F}^{\times}, \quad U_n/U_{n+1} \cong \mathbb{F}^+ \quad (n \geq 1).$$

其中 $\mathbb{F} = \mathbb{O}/\mathfrak{p}$ 是 k 的剩余类域, $U_n = 1 + \mathfrak{p}^n$ ($n \geq 1$). 由于 k'/k 不分歧, 从而 π 也是 k' 的素元. 对于 π 在 k' 中有同样的同构

$$U/U_1 \cong f^*, U'_n/U'_{n+1} \cong f^{*n} \quad (n \geq 1).$$

我们用 T' 和 N' 分别表示有限域扩张 f'/f 的迹和范, 利用定理 4 中的自然同构 $\text{Gal}(k'/k) \cong \text{Gal}(f'/f)$ 即可证得下面两个图表是可交换的:

$$\begin{array}{ccc} U'/U'_1 & \cong & f^{*n} \\ \downarrow N & & \downarrow N \\ U/U_1 & \cong & f^* \end{array} \quad \begin{array}{ccc} U'_n/U'_{n+1} & \cong & f^{*n} \\ \downarrow N & & \downarrow T' \\ U_n/U_{n+1} & \cong & f^{*n} \end{array}$$

此外, 由于有限域扩张 f'/f 中的映射 T' 和 N' 均是满射, 因此两个图表中的竖线 $N = N_{k'/k}$ 也是满射. 从而 $U_n/U_{n+1} (n \geq 0)$ 的每个剩余类中均有 $N_{k'/k}(U'_n)$ 中元素. 然后与证明引理 3 一样得到 $N_{k'/k}(U') = U$.

引理 5 设 k' 是局部域 k 的有限纯不可分扩张, $n = [k':k]$, 则 k'/k 完全分歧并且

$$N_{k'/k}(k') = k'^n = k.$$

证明 如果 k 的特征为 0, 则 $k' = k$, $n = 1$, 从而上述论断都是显然的. 以下设 k 的特征为 p , 于是 n 为 p 的幂. 首先注意 k' 也是局部域, 从而由定理 1 知道 k' 包含一个子域 F 与 k' 的剩余类域 f' 同构, 于是 $k' = F((X))$. 如果 k'/k 是纯不可分扩张, 则对于 k' 中每个元素 x' 均有 $N_{k'/k}(x') = x'^n$. 从而

$$k'^n \subseteq k.$$

由于 F 是特征为 p 的有限域并且 n 为 p 的幂, 从而 $F^n = F$. 于是

$$k'^n = F((X^n)).$$

不难看出 $F((X^n))$ 是 $k' = F((X))$ 的子域并且 $[F((X)): F((X^n))] = n$, 从而由 $[k':k] = n$ 和 $k'^n \subseteq k$ 得到 $k = k'^n$. 此外, 由 $f' \cong F \subseteq k$ 可知 k 的剩余类域 f 与 f' 相同, 从而 $f = [f':f] = 1$, 即 k'/k 是完全分歧的. (从定理 5 也可以得出完全分歧性.)

定理 7 设 k' 是局部域 k 的任意有限扩张, 则 k'/k 的范群 $N_{k'/k}(k'^{\times})$ 和单范群 $N_{k'/k}(U')$ 均是 k^{\times} 的开子群从而也是闭子群, 并且

$$[k^x: N_{k',k}(k'^x)] < +\infty, [U: N_{k',k}(U')] < +\infty.$$

证明 为简单起见, 令 $i(k'/k) = [U: N_{k',k}(U')]$. 先证 $i(k'/k)$ 是有限的. 先设 k'/k 是素数次循环扩张, 则 k'/k 或者不分歧, 或者完全分歧, 分别利用引理 4 或者 §1.4, 定理 5 即知 $i(k'/k) < +\infty$. 又若 k 的特征为 p 而 k'/k 是 p 次纯不可分扩张, 则由引理 5 可知 $i(k'/k) = [U: N_{k',k}(k'^x) \cap U] = 1$. 最后设 k'/k 是任意有限扩张, 设 k'' 为 k'/k 的中间域, U'' 为 k'' 的单位群, 则

$$N_{k',k''}(U') \subseteq U'', N_{k'',k}(U') \subseteq N_{k'',k}(U'') \subseteq U,$$

$$[N_{k'',k}(U''): N_{k',k}(U')] \leq [U'': N_{k',k''}(U'')],$$

从而得到

$$i(k'/k) \leq i(k'/k'')i(k''/k), i(k''/k) \leq i(k'/k).$$

于是由 $i(k'/k'') < +\infty$ 和 $i(k''/k) < +\infty$ 可以推得 $i(k'/k) < +\infty$. 反之由 $i(k'/k) < +\infty$ 也可推出 $i(k''/k) < +\infty$. 由此及定理 6 即可对于任意有限扩张 k'/k 证明 $i(k'/k) < +\infty$, 方法与证明定理 1 一样.

由于 $N_{k',k}(U')$ 紧, 从而为 U 的闭子群. 又由于 $i(k'/k) < +\infty$, 从而它也是 U 的开子群. 又因为 U 是 k^x 的开子群, 所以 $N_{k',k}(U')$ 也是 k^x 的开子群. 由于 $N_{k',k}(k'^x)$ 包含 $N_{k',k}(U')$, 从而自然是 k^x 的开子群. 设 π 是 k 的素元, 由于 $n \in [k':k]$, 从而 $\pi^n \in N_{k',k}(\pi) \in N_{k',k}(k'^x)$. 再由 $k^x = \langle \pi \rangle \times U$ 和 $i(k'/k) < +\infty$ 即得到 $[k^x: N_{k',k}(k'^x)] < +\infty$.

为了今后的需要, 我们举一个单位范群的重要例子作为说明. 以下设 (k, v) 是特征为 p 的 p 局部域. 根据定理 1, k 包含一个有限子域 F 同构于 k 的剩余类域 $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$, 并且 $k = F((X)), \mathfrak{o} = F[[X]], \mathfrak{p} = (X) = XF[[X]]$. 如上令 $U_n = 1 + \mathfrak{p}^n (n \geq 1)$, 则 $F = F^\times, U = V \times U_1 = F^\times \times U_1$, 从而

$$U^p = F^\times \times U_1^p = F^\times \times (1 + X^p F[[X^p]]).$$

令 $m = [n/p]$, 则

$$[U: U^p U_{n+1}] = [U_1: U_1^p U_{n+1}] = q^{n-pm} (n \geq 1),$$

其中 q 为 \mathfrak{f} 的元素个数, 也就是 F 的元素个数. 对于 k 中每个元

素 x , 令

$$\tau(x) = x^p - x,$$

则 $\tau: k^+ \rightarrow k^+$ 定义出加法群 k^+ 的自同态, 它的核是 k 的素域 F_p 的加法群 F_p^+ . 一般地, 对于任意 $n \geq 0$, 令

$$A_n = X^{-n} F[[X]] = \{x \in k \mid v(x) \geq -n\}, B_n = A_n \cap \tau(k^+).$$

由于 $\tau(F) \subseteq F$, $F_p \subseteq F$, 从而 $[F_p: \tau(F)] = p$. 此外若 $x \in p$, 则

$$y = \sum_{i=0}^{\infty} (-x)^{p^i}$$

在 p 中收敛, 并且满足 $\tau(y) = x$, 从而 $p = \tau(p) \subseteq \tau(k^+)$. 如果 $v(x) < 0$, 则 $v(\tau(x)) = pv(x) < 0$, 于是当 $n = 0$ 时 $A_0 = 0$, $B_0 = 0 \cap \tau(k^+) = \tau(0) = \tau(F) + p$, 从而得到

$$[A_0: B_0] = [F: \tau(F)] = p.$$

另一方面, 如果 $v(x) < 0$ 并且 $p \nmid v(x)$, 由于 $F^p = F$, 从而存在元素 $y \in k$, 使得

$$y = x \bmod \tau(k^+), \quad v(x) < v(y).$$

于是当 $n \geq 1$ 时, A_n/B_n 的每个剩余类均含有形如

$$\sum_{i=-n}^{-1} a_i X^i + a_0, \quad a_i \in F$$

的元素. 并且当 $a_i (i \neq 0)$ 过 F 的全部元素, a_0 过 $F/\tau(F)$ 的代表系时, 由上式得到的全部元素即是 A_n/B_n 的完全代表系. 从而

$$[A_n: B_n] = pq^{n-m}, \quad m = [n, p].$$

今后我们需要这个结果.

现在固定 k 的一个代数封闭域 Q , 对于每个元素 $x \in k$, 以 k_x 表示多项式 $Y^p - Y - x$ 在 k 上的分裂域 ($\subseteq Q$). 设 α 是 $Y^p - Y - x$ 的一个根, 则全部根为 $\alpha, \alpha + 1, \dots, \alpha + p - 1$, 从而

$$k_x = k(\alpha), \quad \alpha^p - \alpha = x, \quad \alpha \in Q.$$

关于这种扩张有熟知的 Artin-Schreier 定理, 其结果如下所述:

1) 如果 $x \in \tau(k^+)$, 则 $k_x = k$. 如果 $x \notin \tau(k^+)$, 则 k_x/k 是 p 次循环扩张, $\text{Gal}(k_x/k)$ 是由满足 $\sigma(\alpha) = \alpha + 1$ 的自同构 σ 生成

的,并且(包含在 Ω 中的) k 的每个 p 次循环扩张均可以如此得到.

2) 如果 $x, y \in k, \text{且 } k_x = k_y$ 的充要条件是 x 和 y 在 $k^+/\mathfrak{r}(k^+)$ 中生成同样的子群.

如果 $x \in A_0 + \mathfrak{r}(k^+)$, 由上可知存在 $a \in F$ 使得 $x = a \bmod \mathfrak{r}(k^+)$, 从而 $k_x = k_a = k(\alpha_0)$, 其中 $\alpha_0^p - \alpha_0 = a$. 如果 $a \in \mathfrak{r}(F)$, 则 $\alpha_0 \in F$, 从而 $k_x = k_a = k$. 另一方面, 如果 $a \notin \mathfrak{r}(F)$, 则对于 F 利用 Artin-Schreier 定理, 可知 $F(\alpha_0)/F$ 是 p 次循环扩张, 因而

$$k_x = k_a = F(\alpha_0)((X))$$

是 $k = F((X))$ 的 p 次不分歧扩张(参见前节的例子). 其次, 如果 $x \notin A_0 + \mathfrak{r}(k^+)$, 则由 1) 和 2) 知道 k_x 是 k 的 p 次循环扩张但是不同于上述的不分歧扩张 $k_a = F(\alpha_0)((X))$. 根据定理 4, Ω 中 k 的 p 次不分歧扩张是唯一的, 因此 k_x/k 是分歧扩张, 因此是 p 次完全分歧扩张.

引理 6 设 x 是上面定义加法群 $A_n (n \geq 0)$ 中任意元素, $k' = k_x = k(\alpha)$, $\alpha^p - \alpha = x$, 则

$$U_{n+1} \subseteq N_{k',k}(U'),$$

其中 U' 是 k' 的单位群

证明 先设 $x \in A_0 + \mathfrak{r}(k^+)$, 即 $x \in A_0 + B_n$, 则由上面所述可知 $k' = k_x = k$ 或者 k'/k 是 p 次不分歧扩张. 由引理 4 即知 $N_{k',k}(U') = U$, 从而本引理成立. 以下设 $x \notin A_0 + \mathfrak{r}(k^+)$, 即 $x \notin A_0 + B_n$, 于是 k'/k 是 p 次完全分歧循环扩张. 如果 $k' = k_x$, 则 x 只依赖于 A_n/B_n 的剩余类, 根据上面对于 A_n/B_n 的代表系所作的注记, 我们可以假定

$$v(x) = -i, \quad 1 \leq i \leq n, \quad p \nmid i.$$

设 v' 为 k' 的正规赋值, π' 为 k' 的素元, σ 为如前所述的 $\text{Gal}(k_x/k)$ 的生成元, 则

$$v'(\sigma(\pi') - \pi') = i,$$

即

$$\sigma(\pi') = \pi' + \beta \pi'^p, \quad \beta \in k', \quad v'(\beta) = 0.$$

则由定理 5 可知

$$U_s \subset N_{k'/k}(U).$$

由于 $s = 1$ 时 $U_{s+1} \subset U_s$, 从而引理成立. 以下假定 $s \geq 2$, 则由上述可得

$$\sigma(x'^{-1}) \equiv x'^{-1}(1 - i\beta x'^{-1}) \pmod{x'^{-i+s}},$$

$$\sigma(x'^{-i+1}) \equiv x'^{-i+1} \pmod{x'^{-i+s}} \quad (i \geq 1).$$

另一方面, 由 $\alpha^p - \alpha = x$, $v'(x) = pv(x) = -ip$ 可知 $v'(\alpha) = -i$. 此外, 由于 k'/k 是完全分岐的, 因而 k' 的剩余类域 \bar{k}' 等于 k 的剩余类域 \bar{k} , 从而 \mathbf{F} 也是 \bar{k} 的完全代表系. 所以由 §1.3, 定理 1 可知在 k' 中 α 展开成如下形式

$$\alpha = a_{-i}x'^{-i} + a_{-i+1}x'^{-i+1} + \cdots, a_{-i}, \in \mathbf{F}, a_{-i} \neq 0.$$

再由先前的同余式即得

$$\sigma(\alpha) \equiv \alpha - ia_{-i}\beta x'^{-i+i-1} \pmod{x'^{-i+s}},$$

从 $p \nmid i$, $a_{-i} \in \mathbf{F}$, $a_{-i} \neq 0$ 和 $v'(\beta) = 0$ 得

$$v'(\sigma(\alpha) - \alpha) = -i + s - 1.$$

但是 $\sigma(\alpha) = \alpha + 1$, 所以上式左边的赋值必然是 0, 因此

$$s = i + 1.$$

于是由 $i \leq n$ 即得出

$$U_{s+1} \subset U_s \subset N_{k'/k}(U).$$

这就证明了引理.

第四章 极大不分歧扩域

我们在前章 §3.2 中已经叙述了关于局部域有限扩域的基本性质。为了以后几章作准备,本章要考查 k 的无限扩域,特别是 k 的极大不分歧扩域,同时还证明以后需要的一些有关结果。

§ 4.1 代数扩域和它的范群

本书从此以后均是以局部域 k 作为基域,考查它的代数扩域特别是 Abel 扩域。为方便起见,我们固定 k 的一个代数闭包 \bar{Q} 。由于 \bar{Q}/k 是代数扩张,根据 §1.2, 引理 2 可知 k 的完备正规赋值 ν 可以唯一地扩充为 \bar{Q} 的赋值 μ 。令 \bar{Q} 是 \bar{Q} 对于 μ 的完备化,记 $\bar{\mu}$ 为 μ 到 \bar{Q} 上的自然扩充。这时,若 F 是 k 上任意代数扩域,则不计 k -同构, F 可以看作是 \bar{Q}/k 的中间域。 \bar{Q} 对于 $\bar{\mu}$ 诱导出的拓扑是拓扑域。而 F 在 \bar{Q} 中的闭包 \bar{F} 是 \bar{Q} 的子域。显然 \bar{F} 是 F 对于限制赋值 $\mu|_F$ 的完备化。以下设 F/k 是代数扩张。如上所述我们考虑

$$k \subset F \subset \bar{Q}, \quad k \subseteq F \subseteq \bar{F} \subset \bar{Q},$$

以及

$$\nu_F = \mu|_F, \quad \nu_{\bar{F}} = \bar{\mu}|_{\bar{F}}.$$

ν_F 是 ν 到 k 的代数扩域 F 上的唯一扩充,而 $\nu_{\bar{F}}$ 恰好是 ν_F 到完备化域 \bar{F} 中的自然扩充。

现在设 σ 是 F 的 k 自同构,则由 §1.2, 引理 3 可知 σ 也是 F 的拓扑自同构,并且满足

$$\nu_F \circ \sigma = \nu_F.$$

根据连续性, σ 可以唯一地扩充成 \bar{F} 的拓扑自同构,并且 $\bar{\sigma}$ 在 \bar{F} 上满足

$$v_F \circ \sigma = v_F.$$

由于 $e(v_F/v_F) = 1$, 并且 v_F 和 v_F 的剩余类域一致, 因此 σ 和 $\bar{\sigma}$ 在它们的剩余类域中诱导出相同的同构(参见 §1.2, 引理 3).

如果 F 是 k 的 Galois 扩张, 今后将它的 Galois 群 $\text{Gal}(F/k)$ 看成是对于 Krull 拓扑的全不连通紧群¹⁾. 如果 F' 是 F/k 的中间域, 则 $\text{Gal}(F/F')$ 是 $\text{Gal}(F/k)$ 的闭子群. 因为 F/k 是 Galois 扩张, 适当地选取一族 k 的有限 Galois 扩张 $\{k_i\}_{i \in I}$, 可使 F 是这些 $\{k_i | i \in I\}$ 的并(例如可以取包含在 F 中的全部 k 的有限 Galois 扩张). 如果 k_i 和 k_j 属于上述域族, 并且 $k_i \subseteq k_j$, 我们便记成 $i \leq j$. 这时, 限制映射 $\sigma \mapsto \sigma|_{k_i}$ 定义出有限群的满同态

$$\text{Gal}(k_i/k) \rightarrow \text{Gal}(k_j/k).$$

此外, 由于 F 是 $\{k_i\}_{i \in I}$ 之并, 对于任意两个下标 $i_1, i_2 \in I$, 均存在 $i_3 \in I$ 使得 $i_1 \leq i_3, i_2 \leq i_3$. 从而对于 $i \leq j$ 时的上述同态族, 可以定义有限群 $\text{Gal}(k_i/k)$ 的射影极限 $\varprojlim \text{Gal}(k_i/k)$, 并且

从限制映射给出的同态 $\text{Gal}(F/k) \rightarrow \text{Gal}(k_i/k)$ 诱导出自然同构

$$\text{Gal}(F/k) \xrightarrow{\sim} \varprojlim \text{Gal}(k_i/k).$$

此式右边是射影有限群 (profinite group). 由定义可知这是全不连通群, 而上述同构是从紧群 $\text{Gal}(F/k)$ (对于 Krull 拓扑) 到它的射影有限群的拓扑同构. 今后为简单起见, 利用上面的同构, 我们将 $\text{Gal}(F/k)$ 和 $\varprojlim \text{Gal}(k_i/k)$ 看成是一回事, 写成

$$\text{Gal}(F/k) = \varprojlim \text{Gal}(k_i/k).$$

更一般地, 如果 $k \subseteq F' \subseteq F \subseteq \Omega$, 并且 F/F' 是 Galois 扩张, 则 $\text{Gal}(F'/F)$ 同样是射影有限群.

过去我们把局部域或者完备域的单位群记成 U, U', U_k 等. 今后为明确起见, 对于 Ω/k 的每个中间域 F , F 的(即是 v_F 的)单位群写成 $U(F)$, 而 F 的完备化 \bar{F} 的(即是 v_F 的)单位群写

1) 本章以后经常使用 Galois 群的 Krull 拓扑, 射影有限群以及一般的射影极限和归纳极限等, 关于这些现已熟知的概念, 可参照藤崎[5], 附录, 或者 Cassels-Fröhlich [3], 第五章, 第 116-121 页.

成 $U(\bar{F})$.

对于如上所示的每个 F , 扩张 F/k 的范群和单位范群分别定义成

$$N(F/k) = \bigcap_{k'} N_{k',k}(k'^{\times}),$$

$$NU(F/k) = \bigcap_{k'} N_{k',k}(U(k')).$$

其中 k' 均是过满足 $k \subseteq k' \subseteq F$, $[k':k] < +\infty$ 的全部中间域 k' , 而 $N_{k',k}$ 是有限扩张 k'/k 的范. 显然 $N(F/k)$ 和 $NU(F/k)$ 分别是 k^{\times} 和 $U(k)$ 的子群. 特别当 F/k 是有限扩张的时候, 它与 §3.3 中的范群和单位范群是一致的, 并且由 §3.3, 定理 7 可知 $N(F/k)$ 和 $NU(F/k)$ 是 k^{\times} 的闭子群. 此外, 如果 $k \subseteq F' \subseteq F$, 则

$$N(F/k) \subseteq N(F'/k), \quad NU(F/k) \subseteq NU(F'/k).$$

在 §3.3 中已经说过, 对于任意有限扩张 k'/k , 我们有

$$NU(k'/k) = N(k'/k) \cap U(k').$$

对于一般的 F , 见由定义可直接得出

$$NU(F/k) = N(F/k) \cap U(k).$$

引理 1 对于每个自然数 $n \geq 1$, 均有

$$NU(F/k)^n = \bigcap_{k'} N_{k',k}(U(k'))^n.$$

证明 右边显然包含左边. 于是右边的交集必然包含某个元素 u . 对于满足 $k \subseteq k' \subseteq F$, $[k':k] < +\infty$ 的每个中间域 k' , 令 $S(k') = \{v \in N_{k',k}(U(k')) \mid v^n = u\}$. 由假设可知 $S(k')$ 不是空集合, 并且 $S(k')$ 显然是紧群 $U(k')$ 的闭子集合. 又如果 $k \subseteq k_1$, $k_1 \subseteq F$, $[k_1:k] < +\infty$, $[k':k] < +\infty$, 则 $k \subseteq k'k_1 \subseteq F$, $[k'k_1:k] < +\infty$ 并且 $S(k'k_1) \subseteq S(k_1) \cap S(k')$, 再由 $U(k)$ 的紧性可知全体 $S(k')$ 的交集是非空的. 令 w 是这个交集中的元素, 则 $w \in NU(F/k)$, 从而 $u = w^n \in NU(F/k)^n$, 于是证明了引理.

引理 2 假设 $k \subseteq k' \subset F \subset \Omega$, $[k':k] < +\infty$, 则

$$N_{k'/k}(NU(F/k')) = NU(F, k).$$

证明 由于 k'/k 是有限扩张, 从而 k' 也和 k 一样是局部域. 于是可以和定义 $NU(F/k)$ 一样对于代数扩张 F/k' 定义单位范群 $NU(F/k')$. 也就是说, 令 k'' 过满足 $[k'':k'] < +\infty$ 的 F/k' 的全部中间域, 则

$$NU(F/k') = \bigcap_{k''} N_{k''/k'}(U(k'')).$$

另一方面不难看出

$$NU(F, k) = \bigcap_{k''} N_{k''/k}(U(k'')).$$

从而引理中等式的左边包含右边, 于是左边必然包含 $NU(F/k)$ 中任意元素 u . 对每个 k'' , 令

$$S(k'') = \{v \in N_{k''/k'}(U(k'')), N_{k'/k}(v) = u\},$$

与证明上一引理一样地可知 $S(k'')$ 是 $U(k')$ 的非空闭子集, 并且 $S(k'_1 k'_2) \subset S(k'_1) \cap S(k'_2)$. 再由 $U(k')$ 的紧性即知交集 $\bigcap_{k''} S(k'')$ 是非空的. 设 $\omega \in \bigcap_{k''} S(k'')$, 则 $\omega \in NU(F/k')$, 于是 $u = N_{k'/k}(\omega) \in N_{k'/k}(NU(F/k'))$. 这就证明了引理.

§ 4.2 极大不分歧扩域 k_{nr}

$k, \Omega, \bar{\Omega}$ 等如上节所述. 如果 k' 是 k 的有限扩域, 则 $v_{k'} = \mu|_{k'}$ 是 k 的完备正规赋值 v 到 k' 的唯一扩充. 根据 §1.3 的定义我们有

$$e(k'/k) = e(v_{k'}/v) = [v_{k'}(k'^{\times}); v(k^{\times})].$$

从而 k'/k 是不分歧扩张的充要条件是 $v_{k'}(k'^{\times}) = v(k^{\times}) = \mathbf{Z}$, 即 $v_{k'}$ 是正规赋值. 一般地, 对于 k 的任意(不必有限)代数扩域 $F, k \subseteq F \subseteq \Omega$, 如果 $v_F = \mu|_F$ 是正规赋值, 我们就定义 F/k 为不分歧扩张. 如果 F/k 是不分歧扩张而 $k \subset F' \subseteq F$, 则 F'/k 也

是不分歧扩张,

令 f 是局部域 k 的剩余类域, q 为有限域 f 的元素个数. 根据 §3.2, 定理 4, 对于每个自然数 $n \geq 1$, 均存在唯一的中间域 k_n 使得

$$k \subseteq k_n \subseteq Q, [k_n:k] = n, k_n/k \text{ 不分歧.}$$

k_n 即是 $X^{q^n} - X$ 在 k 上的分裂域, 因此 k_n/k 为 n 次循环扩张. 如果以 f_n 表示 k_n 的剩余类域, 则自然映射 $\sigma \mapsto \sigma'$ 给出同构

$$\text{Gal}(k_n/k) \rightarrow \text{Gal}(f_n/f).$$

如果 $n \mid m$, 则 $X^{q^n} - X$ 可以整除 $X^{q^m} - X$, 因此 $k_n \subseteq k_m$. 从而全部 $k_n (n \geq 1)$ 的并集合 K 是 Q/k 的中间域. 由于 $v_K|_{k_n} = \mu|_{k_n} = v_{k_n}$ 是 k_n 上的正规赋值, 从而 $v_K = \mu|_K$ 是 K 上的正规赋值, 即 K/k 是不分歧扩张. 另一方面, 设 F/k 是任意一个不分歧扩张, 取 $\alpha \in F$, 则 $k(\alpha)/k$ 也不分歧, 如果令 $[k(\alpha):k] = n$, 则 $k(\alpha) \subseteq k_n$. 因此 $\alpha \in k_n \subseteq K$, 即 $F \subseteq K$. 换句话说, K 是 (包含在 Q 中的) k 之极大不分歧扩张, 以下将 K 记为 k_{nr} :

$$k_{nr} = K = \bigcup_{n \geq 1} k_n.$$

每个 k_n/k 均是 Abel 扩张, 从而 k_{nr}/k 也是 Abel 扩张. 并且 K 是添加所有多项式 $X^{q^n} - X (n \geq 1)$ 的全部根到 k 中而得到的域, 也即是添加所有 $(q^n - 1)$ 次 $(n \geq 1)$ 单位根到 k 中而得到的域. 设 k 是 p 局部域, 则 q 为 p 的幂, 从而上述单位根全体恰好是 Q 中阶与 p 互素的全体单位根 V_∞ . 也就是说,

$$K = k_{nr} = k(V_\infty).$$

定理 1 $K = k_{nr}$ 的剩余类域 f_K 是 k 的剩余类域 f 的代数闭包. 如果以 σ' 表示元素 $\sigma \in \text{Gal}(K/k)$ 诱导出来的 f_K 的 f -自同构, 则 $\sigma \mapsto \sigma'$ 定义出拓扑同构

$$\text{Gal}(K/k) \xrightarrow{\sim} \text{Gal}(f_K/f).$$

证明 当 $n \mid m$ 时 $k_n \subseteq k_m$, 从而 $f_n \subseteq f_m \subseteq f_K$. 又因为 K 是 $k_n (n \geq 1)$ 之并集合, 从而 K 的赋值环也是 $k_n (n \geq 1)$ 的赋值环的并集合, 并且 f_K 是子域 $f_n (n \geq 1)$ 之并集合. 但是对于每个

自然数 $n \geq 1$, 有限域 f 只有唯一的 n 次扩域, 再加上 $[f_n:f] = [k_n:k] = n$, 从而可知 f_K 是 f 的代数闭包. 此外, 当 $n|m$ 时 $k_n \subseteq k_m$, 限制映射 $\sigma \mapsto \sigma|_{k_n}$ 定义出同态 $\text{Gal}(k_m/k) \rightarrow \text{Gal}(k_n/k)$, 又由于上一节所述可知 K 是 $k_n (n \geq 1)$ 的并集合, 从而

$$\text{Gal}(K/k) = \varprojlim \text{Gal}(k_n/k).$$

完全同样地,

$$\text{Gal}(f_K/f) = \varprojlim \text{Gal}(f_n/f).$$

另一方面, 对于每个 $n \geq 1$, 定理中所述的映射 $\sigma \mapsto \sigma$ 诱导出 §3.2, 定理 4 中的同构 $\text{Gal}(k_n/k) \cong \text{Gal}(f_n/f)$, 然后从上面两个等式即得到

$$\text{Gal}(K/k) \cong \text{Gal}(f_K/f).$$

由于 K/k 是不分歧扩张而 v_K 是正规赋值, 于是 §1.3 中定义的 (K, v_K) 的完备化 $(\bar{K}, v_{\bar{K}})$ 是完备域. 并且 \bar{K} 的剩余类域 \bar{k} 与 K 的剩余类域 k 一致. 又由上述定理知 f_K 是代数封闭域, 从而 $(\bar{K}, v_{\bar{K}})$ 即是在第二章研究过的闭完备域. 这样一来, 我们可以从局部域 k 自然地构造出一个闭完备域. 例如: 设 \bar{F} 为有限域 F 的代数闭包, 则由局部域 $k = F((X))$ 决定出的闭完备域 \bar{K} 恰好是 $\bar{F}((X))$. (参见 §3.2 的例子.)

由于 f 是 q 元有限域而 f_K 是它的代数闭包, 从而映射

$$\omega \mapsto \omega^q, \omega \in f_K$$

是 f_K 的 f 自同构. 由于 $\text{Gal}(K/k) \cong \text{Gal}(f_K/f)$, 对应于上述自同构的 $\text{Gal}(K/k)$ 中元素 φ 叫作扩张 K/k 的 Frobenius 自同构 (或者叫作 Frobenius 置换). 设 \mathfrak{o}_K 和 \mathfrak{p}_K 分别为 K 的赋值环和极大理想, 按照 φ 的定义, 对于 \mathfrak{o}_K 中每个元素 α 均有

$$\varphi(\alpha) = \alpha^q \pmod{\mathfrak{p}_K},$$

并且这个性质唯一地刻画了 $\text{Gal}(K/k)$ 中的 Frobenius 自同构. 对于每个 $n \geq 1$, φ 显然诱导出 k_n/k 的 Frobenius 自同构 φ_n (§3.2). 由于 $\text{Gal}(k_n/k)$ 是由 φ_n 生成 n 阶循环群, 从而

$$\mathbb{Z}/n\mathbb{Z} \cong \text{Gal}(k_n/k),$$

$$a \bmod n \mapsto \varphi_n^a.$$

因此当 $n \mid m$ 时, $\varphi_m|_{k_n} = \varphi|_{k_n} = \varphi_n$, 从而得出交换图表

$$\begin{array}{ccc} \mathbf{Z}/m\mathbf{Z} & \xrightarrow{\sim} & \text{Gal}(k_m/k) \\ \downarrow & & \downarrow \\ \mathbf{Z}/n\mathbf{Z} & \xrightarrow{\sim} & \text{Gal}(k_n/k) \end{array}$$

其中左边竖线是由 $a \bmod m \mapsto a \bmod n$ 定义的自然同态. 设

$$\mathbf{Z} = \varprojlim \mathbf{Z}/n\mathbf{Z}$$

是对 $n \mid m$ 定义的这种同态族的射影极限, 则 $\Gamma = \text{Gal}(K/k) = \varprojlim \text{Gal}(k_n/k)$ 以及上面的交换图表, 即得到射影有限群(即是全不连通的紧群)的拓扑同构

$$\tilde{\mathbf{Z}} \xrightarrow{\sim} \text{Gal}(K/k). \quad (1)$$

自然同态 $\mathbf{Z} \rightarrow \mathbf{Z}/n\mathbf{Z}$ ($n \geq 1$) 诱导出单射 $\mathbf{Z} \rightarrow \tilde{\mathbf{Z}}$, 并且 \mathbf{Z} 是 $\tilde{\mathbf{Z}}$ 的稠子群. 仔细考查上述同构(1)的定义, 可知自然数 $1 \in \mathbf{Z}$ 作为 \mathbf{Z} 中元素, 由同构(1)映成 K/k 的 Frobenius 自同构 φ :

$$1 \mapsto \varphi.$$

于是同构(1)诱导出子群同构

$$\mathbf{Z} \xrightarrow{\sim} \langle \varphi \rangle, \quad n \mapsto \varphi^n.$$

其中 $\langle \varphi \rangle$ 是由 φ 生成的 $\text{Gal}(K/k)$ 的子群, 但是 \mathbf{Z} 在 $\tilde{\mathbf{Z}}$ 中稠密, 从而 $\langle \varphi \rangle$ 为 $\text{Gal}(K/k)$ 的稠子群. 因此拓扑同构(1)由条件 $1 \mapsto \varphi$ 所唯一决定.

注记 设 p 是素数, \mathbf{Z}_p^* 为 p -adic 加法群, 则上面的 $\tilde{\mathbf{Z}}$ 同构于直积 $\prod_p \mathbf{Z}_p^*$, 从而是紧群.

从定理 1 的证明我们知道, \mathbf{f}_K 为 \mathbf{f}_n ($n \geq 1$) 的并集合. 将 §3.1, 引理 1 的系用于 k_n ($n \geq 1$), 可知自然同态 $\mathbf{o}_K \rightarrow \mathbf{f}_K = \mathbf{o}_K/\mathbf{p}_K$ 诱导出乘法群的同构

$$V_\infty \xrightarrow{\sim} \mathbf{f}_K^*.$$

其中 V_∞ 即是早先定义的阶与 q 互素(即是与 p 互素)的单位根全体. 从而 $\varphi(V_\infty) = V_\infty$, 但是 Frobenius 自同构 φ 对于 V_∞ 中

元素 η 满足同余式 $\varphi(\eta) = \eta^q \pmod{p_K}$, 从而必然满足等式

$$\varphi(\eta) = \eta^q, \eta \in V_{\infty}.$$

现在证明关于 $K = k_{\infty}$ 和它的完备化 \bar{K} (即 K 在 $\bar{\mathcal{Q}}$ 中的闭包) 的一些结果. 根据上节的记号, K/k 的 Frobenius 自同构 φ 唯一地扩充成 K 的自同构 $\bar{\varphi}$, 并且 φ 和 $\bar{\varphi}$ 在剩余类域 $\mathfrak{f}_K = \mathfrak{f}_{\bar{K}}$ 上诱导出同样的自同构 $\omega \mapsto \omega^q$. 为简单起见, 今后若不会发生误解, 我们也将 $\bar{\varphi}$ 写成 φ . 设

$$\mathfrak{f} = \mathfrak{o}/\mathfrak{p}, \mathfrak{f}_K = \mathfrak{o}_K/\mathfrak{p}_K,$$

则 \bar{K} 的自同构 $\varphi (= \bar{\varphi})$ 显然诱导出赋值环 $\mathfrak{o}_{\bar{K}}$ 的加法群以及单位群 $U(\bar{K})$ 的下列自同态:

$$\varphi - 1: \mathfrak{o}_{\bar{K}} \rightarrow \mathfrak{o}_{\bar{K}}, \alpha \mapsto (\varphi - 1)\alpha = \varphi(\alpha) - \alpha,$$

$$\varphi - 1: U(\bar{K}) \rightarrow U(\bar{K}), \xi \mapsto \xi^{\varphi-1} = \varphi(\xi)/\xi.$$

关于它们有如下定理:

定理 2 设 $\mathfrak{o} \rightarrow \mathfrak{o}_K, U(k) \rightarrow U(K)$ 是自然单射, 则下面是两个正合序列

$$0 \rightarrow \mathfrak{o} \rightarrow \mathfrak{o}_{\bar{K}} \xrightarrow{\varphi-1} \mathfrak{o}_K \rightarrow 0,$$

$$1 \rightarrow U(k) \rightarrow U(K) \xrightarrow{\varphi-1} U(K) \rightarrow 1.$$

证明 我们只叙述第二个序列的正合性证明, 第一个序列可以类似地证明. 首先, 由于 $\mathfrak{f}_{\bar{K}} = \mathfrak{f}_K$ 是代数封闭域, 因此 $\omega \mapsto \omega^q = \omega, \omega \mapsto \omega^{\varphi-1}$ 分别将 $\mathfrak{f}_{\bar{K}}$ 和 \mathfrak{f}_K 映到其自身之上, 于是得到

$$(\varphi - 1)\mathfrak{o}_K + \mathfrak{p}_K = \mathfrak{o}_K, U(\bar{K})^{\varphi-1}(1 + \mathfrak{p}_K) = U(K). \quad (2)$$

此外, 由于 K/k 不分歧, 从而 k 的素元 π 同时也是 K 的素元, 因此也是 K 的素元.

如果 $\xi \in U(k)$, 则显然 $\xi^{\varphi-1} = 1$. 反之, 假设 $\xi \in U(\bar{K}), \xi^{\varphi-1} = 1$, 即 $\varphi(\xi) = \xi$. 由于 $\mathfrak{f}_{\bar{K}} = \mathfrak{f}_K$, 可知上述集合 V_{∞} 与零元素 0 的并集合 A 构成 $\mathfrak{f}_{\bar{K}}$ 在 $\mathfrak{o}_{\bar{K}}$ 的完全代表系. 将 §1.3, 定理 1 用于完备域 \bar{K} , 可知 ξ 唯一地展成

$$\xi = \sum_{n=0}^{\infty} a_n \pi^n, a_n \in A.$$

由 $\pi \in k$, 从而 $\varphi(\pi) = \pi$, 但是 V_∞ 中 (从而 A 中) 每个元素 a 均有 $\varphi(a) = a^q \in A$. 因此

$$\begin{aligned}\xi = \varphi(\xi) &= \sum_{n=0}^{\infty} \varphi(a_n) \varphi(\pi)^n \\ &= \sum_{n=0}^{\infty} a_n^q \pi^n, \quad a_n^q \in A.\end{aligned}$$

由展开的唯一性可知

$$a_n^q = a_n \quad (n \geq 0).$$

于是由 §3.1, 引理 1 即知 $a_n \in k$ ($n \geq 0$). 但是局部域 k 是完备的, 因此 $\xi = \sum_{n=0}^{\infty} a_n \pi^n \in k$, 从而 $\xi \in U(k) = k^\times \cap U(\bar{K})$. 这就证明了

$$1 \rightarrow U(k) \rightarrow U(\bar{K}) \xrightarrow{\varphi-1} U(\bar{K})$$

的正合性.

其次, 对于任意元素 $\xi \in U(\bar{K})$, 我们现在证明存在 $U(\bar{K})$ 中元素序列 $\{\eta_n\}_{n \geq 0}$ 使得

$$\xi = \eta_0^{\varphi-1} \bmod p_K^{\varphi+1}, \quad \eta_n \equiv \eta_{n+1} \bmod p_K^{\varphi+1} \quad (n \geq 0).$$

由(2)式显然得出 η_0 的存在性. 现在假定满足条件的 $\eta_0, \eta_1, \dots, \eta_n$ ($n \geq 0$) 已经作出, 并设 $\xi \eta_n^{1-\varphi} = 1 + \alpha \pi^{\varphi+1}$, 其中 $\alpha \in \mathfrak{o}_K$. 由(2)式可知存在 $\beta \in \mathfrak{o}_K$, 使得 $\alpha \equiv (\varphi - 1)\beta \bmod p_K$. 对于这个 β 我们令 $\eta_{n+1} = \eta_n(1 - \beta \pi^{\varphi+1})$, 则 $\eta_{n+1} \in U(\bar{K})$ 并且直接验证有:

$$\xi = \eta_{n+1}^{\varphi-1} \bmod p_K^{\varphi+2}, \quad \eta_n \equiv \eta_{n+1} \bmod p_K^{\varphi+1}.$$

这就证明了 $\{\eta_n\}_{n \geq 0}$ 的存在性. 由于 \bar{K} 是完备域, 从而 $\{\eta_n\}_{n \geq 0}$ 在 K 中收敛. 令

$$\eta = \lim_{n \rightarrow \infty} \eta_n,$$

则 $\eta \in U(\bar{K})$ 并且显然有 $\xi = \eta^{\varphi-1}$. 于是 $U(\bar{K}) \xrightarrow{\varphi-1} U(\bar{K})$ 是满射. 这就证明了定理.

引理 3 对于 $K = k_{ur}$ 我们有

$$N(K/k) = NU(K/k) = U(k).$$

证明 从 §3.3, 引理 4 知道, 对于每个 $n \geq 1$ 均有 $N_{k_n/k}(U(k_n)) = U(k)$. 因为 K 是 $k_n (n \geq 1)$ 之并集, 从而由定义直接得到 $NU(K/k) = U(k)$. 此外, k 的素元 π 也是 k_n 的素元并且 $k_n^\times = \langle \pi \rangle \times U(k_n)$, 从而

$$N_{k_n/k}(k_n^\times) = \langle \pi^n \rangle \times U(k).$$

再由 $\langle \pi \rangle \simeq \mathbf{Z}$ 即得到 $N(K/k) = U(k)$.

引理 4 设 F 是 k 的代数扩域, 即 $k \subseteq F \subseteq \Omega$, 则范群 $N(F/k)$ 包含 k 的素元的充要条件是

$$F \cap K = k, \quad K = k_{ur}.$$

证明 如果 $F \cap K \neq k$, 则存在适当的 $n \geq 2$ 使得 $k_n \subseteq F \cap K$. 从上一引理的证明可知 $N(F/k) \subseteq N(k_n/k) = \langle \pi^n \rangle \times U(k)$, 所以当 $n \geq 2$ 时 $N(F/k)$ 不包含 k 的素元. 另一方面, 如果 $F \cap K = k$, 设 k' 为包含在 F 中的 k 之任意有限扩域, 以 $\Pi_{k'}$ 表示 k' 的素元全体. 如果 $\pi' \in \Pi_{k'}$, 则 $\Pi_{k'} = \pi' U(k')$, 从而 $\Pi_{k'}$ 是 k' 的紧子集. 此外, 由于 $k' \cap K = k$ 可知 k'/k 是完全分歧的, 从而 $N_{k'/k}(\pi')$ 是 k 的素元, 即 $N_{k'/k}(\pi') \in \Pi_k$. 如果令

$$S(k') = N_{k'/k}(\Pi_{k'}) = N_{k',k}(\pi') NU(k'/k),$$

则 $S(k')$ 是 Π_k 的非空紧子集合, 并且与证明上节引理 1 一样可以得到 $S(k_1 k_2) \subseteq S(k_1) \cap S(k_2)$. 从而由 Π_k 的紧性可知 $S(k')$ (对于全体 k') 的交集也是非空的. 设 π 是这个交集集合中的元素, 则 π 显然为 k 的素元并且属于 $N(F/k)$. 从而证明了引理.

§ 4.3 $K = k_{ur}$ 的扩域

现在证明关于 $K = k_{ur}$ 的扩域特别是有限扩域的一些引理.

引理 5 设 L 是 $K = k_{ur}$ 的任意有限扩域, 则存在 k 的有限扩域 k' 使得

$$L = k'K.$$

并且对于这样的 k' , 我们有

$$L = k'_{ur} = k' \text{ 的极大不分歧扩域,}$$

$$N(L/k) = NU(L/k) = NU(k'/k).$$

从而 L 的完备化 \bar{L} 与 K 一样是闭完备域.

证明 设 $L = K(\alpha_1, \dots, \alpha_n)$, 令 $k' = k(\alpha_1, \dots, \alpha_n)$, 则 k'/k 是有限扩张并且 $L = k'K$. 由 §4.2 的注记可知 $K = k(V_\infty)$, 从而

$$L = k'K = k'(V_\infty) = k'_{ur}.$$

此外, 由引理 3 可知 $N(L/k) \subseteq N(K, k) = U(k)$, 从而

$$N(L/k) = N(L/k) \cap U(k) = NU(L/k).$$

另一方面, 将引理 2 和引理 3 用于 $L = k'_{ur}$ 可知

$$\begin{aligned} NU(L/k) &= N_{k',k}(NU(L/k')) \\ &= N_{k',k}(U(k')) = NU(k'/k). \end{aligned}$$

最后由于 $L = k'_{ur}$, 从而 \bar{L} 与 \bar{K} 一样是闭完备域.

引理 6 设 L 是 $K = k_{ur}$ 的有限可分扩域, 则

$$\bar{K}L = \bar{L}, \bar{K} \cap L = K, [\bar{L}:\bar{K}] = [L:K].$$

特别若 L/K 是有限 Galois 扩张, 则 \bar{L}/\bar{K} 也是 Galois 扩张, 并且映射 $\bar{\sigma} \mapsto \sigma = \bar{\sigma}|L$ 给出同构

$$\text{Gal}(\bar{L}/\bar{K}) \xrightarrow{\sim} \text{Gal}(L/K).$$

证明 从 $L \subseteq \bar{K}L \subseteq \bar{L}$ 不难看出 $\bar{K}L$ 在 \bar{L} 中稠密, 而 $\bar{K}L/\bar{K}$ 是有限扩张, 从而由 §1.2, 引理 2 可知 \bar{K} 的完备赋值 $v_{\bar{K}} = \bar{\mu}|_{\bar{K}}$ 在 $\bar{K}L$ 中的扩充 $\bar{\mu}|_{\bar{K}L}$ 是完备的. 所以 $\bar{K}L$ 对于由 $v_L = \bar{\mu}|_{\bar{L}}$ 决定的拓扑是 \bar{L} 的闭集, 因此 $\bar{K}L = \bar{L}$.

其次, 设 L' 是 K 的有限 Galois 扩域并且包含 L , 则 $K \subseteq \bar{K} \cap L \subseteq \bar{K} \cap L'$. 因此为证 $K \cap L = K$, 不妨假定 L/K 是 Galois 扩张, 从而 $\bar{L}/\bar{K} = \bar{K}L/\bar{K}$ 也是 Galois 扩张. 由 §4.1 中的注记可知 $\text{Gal}(L/K)$ 中每个元素 σ 均可以扩充成 $\text{Gal}(\bar{L}/\bar{K})$ 中元素 $\bar{\sigma}$: $\bar{\sigma}|L = \sigma$. 从而 $\text{Gal}(L/K)$ 的阶数不超过 $\text{Gal}(\bar{L}/\bar{K})$ 的阶数. 另一方面, 再由 $[\bar{L}:\bar{K}] = [\bar{K}L:\bar{K}] = [L:\bar{K} \cap L] \leq [L:K]$ 即知 $\bar{K} \cap L = K$. 并且 $\bar{\sigma} \mapsto \sigma = \bar{\sigma}|L$ 给出同构 $\text{Gal}(\bar{L}/\bar{K}) \xrightarrow{\sim} \text{Gal}(L/K)$.

$K)$.

系 设 Ω_i 为 k 在 Ω 中的极大可分扩域, 则

$$\bar{K} \cap \Omega_i = K.$$

证明 首先注意

$$k \subset K = k_{\text{sep}} \subset \Omega_i \subset \Omega \subset \bar{\Omega},$$

根据引理 6, Ω_i 是 K 的全部有限可分扩域 L 之和, 然后由 $\bar{K} \cap L = K$ 即得出 $\bar{K} \cap \Omega_i = K$.

一般地, 若 L 是 $K = k_{\text{sep}}$ 的任意代数扩域, 如果 L/k 的中间域 k' 满足

$$k' \cap K = k, k'K = L,$$

我们将 k' 叫作 L/k 的补域. 由于 K/k 是 Galois 扩域, 从而若 k' 为补域, 则 L/k' 也是 Galois 扩张, 并且

$$[L:K] = [k':k], \text{Gal}(L/k') \cong \text{Gal}(K/k).$$

特别若 L/K 是有限扩张, 则 k', k 也是有限扩张, 这时由引理 5 可知 $L = k'_{\text{sep}}$. 令 k, k', K, L 的剩余类域分别为 $\bar{k}, \bar{k}', \bar{k}_K, \bar{k}_L$, 则由上节可知 \bar{k}_K 和 \bar{k} 分别为 \bar{k}' 和 \bar{k} 的代数闭包. 由定义知 $k' \cap K = k$, 即 k'/k 是完全分歧的, 从而 $\bar{k} = \bar{k}'$, 于是

$$\bar{k}_K = \bar{k}_L.$$

如果 φ, φ' 分别是 K/k 和 L/k' 的 Frobenius 自同构, 则由定义直接得到

$$\varphi'K = \varphi.$$

于是存在自然同构 $\text{Gal}(L/k') \cong \text{Gal}(K/k)$ 使得 $\varphi' \mapsto \varphi$.

现在证明补域的存在性. 一般来说, 设 N 是射影有限群 G 的正规闭子群, 作为紧群我们有同构

$$G/N \cong \tilde{Z} = \varprojlim \tilde{Z}/n\tilde{Z}. \quad (3)$$

取定 G 中元素 σ 使得在上述同构下有 $\sigma N \mapsto 1$. 以 H 表示 G 中由 σ 生成的循环群 $\langle \sigma \rangle$ 的闭包, 我们有

$$f: \tilde{Z} \rightarrow \langle \sigma \rangle, n \mapsto \sigma^n.$$

与 G 一样, H 也是射影有限群, H 的开 (正规) 子群集合 $\{U\}$ 形成

1 在 H 中的基本邻域系, 其中对每个这样的 U , 如果令 $m = [H:U]$, 则 m 是有限的, 从而

$$f(m\mathbf{Z}) \subseteq \langle \sigma \rangle \cap U.$$

从而 $f: \mathbf{Z} \rightarrow \langle \sigma \rangle$ 可以扩充成连续满同态

$$f: \tilde{\mathbf{Z}} \rightarrow H,$$

于是再往自然的单射 $H \rightarrow G$, 便得到序列

$$G/N \xrightarrow{\sim} \tilde{\mathbf{Z}} \rightarrow H \rightarrow G \rightarrow G/N,$$

$$\sigma N \mapsto 1 \mapsto \sigma \mapsto \sigma \mapsto \sigma N.$$

因此, 自然满射 $G \rightarrow G/N$ 诱导出拓扑同构

$$H \xrightarrow{\sim} G/N.$$

于是有

$$HN = G, H \cap N = 1. \quad (4)$$

反之, 如果 G 的闭子群 H 满足 (4) 中两个等式, 这时 $G \rightarrow G/N$ 诱导出同构 $H \xrightarrow{\sim} G/N$, 因此有

$$H \xrightarrow{\sim} G/N \xrightarrow{\sim} \tilde{\mathbf{Z}},$$

假设在这些同构中, $\sigma \mapsto \sigma N \mapsto 1$, 则 H 即为循环群 $\langle \sigma \rangle$ 在 G 中的闭包. 于是由同构 (3) 可知 $\sigma N \rightarrow 1$ 给出 G 中元素 σ 和满足 (4) 式的 G 的闭子群 H 之间的一一对应.

引理 7 设 L 是 k 的 Galois 扩张并且包含 $K = k_{nr}$, 则存在 L/k 的补域 $k': k' \cap K = k, k'K = L$. 事实上, 令 ϕ 是 K/k 的 Frobenius 自同构 φ 扩充成的 L/k 的一个自同构, 则 L 中的 ϕ 不变元素全体组成的域 k' 即是 L/k 的补域, 并且

$$\phi \mapsto k'$$

给出 φ 的扩充 ϕ 组成的集合与 L/k 的补域集合之间的一一对应.

证明 首先注意, 由于 L/k 是 Galois 扩张, 从而 φ 可以扩张成 L/k 的自同构. 令 $G = \text{Gal}(L/k)$, $N = \text{Gal}(L/K)$, 则由 (1) 式给出

$$G/N = \text{Gal}(K/k) \xrightarrow{\sim} \tilde{\mathbf{Z}},$$

$$\varphi \mapsto 1.$$

从而 $G = \text{Gal}(L/k)$ 中元素 ϕ 是 φ 的扩充相当于说 $\phi N = \varphi$. 根据 Galois 理论, 引理中的 k' 恰好是 $\langle \phi \rangle$ 在 G 中的闭包所对应的 L/k 的中间域. 所以立刻从上述群论方面(取 $\sigma = \phi$) 的结果证得引理的论断.

第五章 Abel 扩张 k_{ab}/k_{ur}

我们继续沿用前章的记号, 固定局部域 k 的代数闭包 \bar{Q} 和它的完备化 \bar{Q} , 则 k 的代数扩张 F 和它的完备化 \bar{F} 分别看成是 \bar{Q} 和 \bar{Q} 的子域. 如果以 k_{ab} 表示包含在 \bar{Q} 之中的 k 的全部 Abel 扩张的合成域, 则 k_{ab} 自身也是 k 的 Abel 扩张. 因此我们将 k_{ab} 叫作(包含在 \bar{Q} 中的) k 的极大 Abel 扩张. 由于 k 的极大不分歧扩张 k_{ur} 是 k 的 Abel 扩张 (§4.2), 因此 k_{ur} 是 k_{ab} 的子域:

$$k \subseteq k_{ur} \subseteq k_{ab}.$$

上章我们叙述了扩张 $K/k (=K/k)$. 在本章中, 我们首先介绍 [Hazewinkel [6]] 中的基本思想的一般形式, 然后用由此得到的结果来研究 Abel 扩张 k_{ab}/k_{ur} , 特别地, 我们要证明存在着从 k 的单位群 $U(k)$ 到 Galois 群 $\text{Gal}(k_{ab}/k_{ur})$ 的自然拓扑同构 δ_k .

§ 5.1 有限 Galois 扩张 E/k

设 E 是局部域 k 的任意有限 Galois 扩张, 而令

$$K = k_{ur}, \quad k_0 = E \cap K, \quad L = EK.$$

于是 k_0 是包含在 E 中的 k 的极大不分歧扩张, 即是 E/k 的惯性域 (§3.2). 另一方面, 由 §4.3 的引理 5 知道

$$L = E_{ur} = E \text{ 的极大不分歧扩张,}$$

$$[L:K] < +\infty.$$

并且 K 和 L 的完备化 \bar{K} 和 \bar{L} 均为闭完备域. 由于 E/k 和 K/k 都是 Galois 扩张, 从而 L/K 也是 Galois 扩张, 再由 §4.3, 引理 6 知道完备化的扩张 \bar{L}/\bar{K} 也是 Galois 扩张, 并且限制映射 $\sigma \mapsto \bar{\sigma} = \sigma|_{\bar{L}}$ 给出同构 $\text{Gal}(\bar{L}/\bar{K}) \cong \text{Gal}(L/K)$. 今后为简单起见, 我们将 $\bar{\sigma}$ 和 σ 视为等同, 从而

$$\text{Gal}(\bar{L}/\bar{K}) = \text{Gal}(L/K).$$

象 §4.1 中那样,令 $U(\bar{K})$ 和 $U(\bar{L})$ 分别是 \bar{K} 和 \bar{L} 的单位群. 但是今后把 §2.2 中定义的 $U(\bar{L})$ 之子群 $\downarrow_{\bar{L}/\bar{K}}$ 写成 $V(\bar{L}/\bar{K})$. 换句话说, $V(L/\bar{K})$ 是由 $\{\xi^{\sigma-1} = \sigma(\xi)/\xi \mid \xi \in U(\bar{L}), \sigma \in \text{Gal}(L/K)\}$ 生成的子群. 由于 \bar{L}/\bar{K} 是闭完备域的有限 Galois 扩张, 从而由 §2.2, 定理 2 有基本正合序列

$$\begin{aligned} 1 \rightarrow \text{Gal}(L/K)^{\text{ab}} &\xrightarrow{i} U(\bar{L})/V(\bar{L}/\bar{K}) \\ &\xrightarrow{N} U(\bar{K}) \rightarrow 1. \end{aligned} \quad (1)$$

其中 i 是由 §2.2, 定理 4 中的 $i: \text{Gal}(L/K) \rightarrow U(\bar{L})/V(\bar{L}/\bar{K})$ 诱导出来的同态, 而 $N = N_{\bar{L}/\bar{K}}$ 是 \bar{L}/\bar{K} 的范映射.

令 φ_0 和 ϕ 分别是 K/k_0 和 L/E 的 Frobenius 自同构, 由于 E 是 L/k_0 的闭域, 从 §4.3 的注记我们得到

$$\phi(K) = \varphi_0.$$

如果 ρ 是 $\text{Gal}(L/k)$ 中任意元素, 则 $\rho\phi\rho^{-1}$ 显然是 $\rho(L)/\rho(E)$ 的 Frobenius 自同构. 但是 $\rho(L) = L$, $\rho(E) = E$, 所以

$$\rho\phi\rho^{-1} = \phi, \text{ 即 } \rho\phi = \phi\rho.$$

如果将 ρ 和 ϕ 均看成是它们扩充成的 \bar{L} 的自同态, 则上面等式也成立. 特别地, 对于每个 $\sigma \in \text{Gal}(L/K)$ 和 $\xi \in U(\bar{L})$, 我们有

$$(\xi^{\sigma-1})^{\phi-1} = (\xi^{\phi-1})^{\sigma-1}.$$

但是根据 §4.2, 定理 2 知道 $\phi - 1: U(\bar{L}) \rightarrow U(\bar{L})$ 是满射, 从而由上式给出

$$V(\bar{L}/K)^{\phi-1} = V(\bar{L}/\bar{K}). \quad (2)$$

即 $\phi - 1: V(\bar{L}, \bar{K}) \rightarrow V(L/\bar{K})$ 是满射. 特别地, 同态 $\phi - 1: U(\bar{L}) \rightarrow U(\bar{L})$ 诱导出自同态

$$\begin{aligned} \alpha = \phi - 1: U(\bar{L})/V(\bar{L}/\bar{K}) \\ \rightarrow U(\bar{L})/V(\bar{L}/\bar{K}). \end{aligned}$$

其次令

$$\beta = \varphi_0 - 1: U(\bar{K}) \rightarrow U(\bar{K}).$$

又设

$$\gamma: \text{Gal}(L/K)^{ab} \rightarrow \text{Gal}(L/K)^{ab}$$

是 $\text{Gal}(L/K)^{ab}$ 的平凡自同态, 即 γ 将 $\text{Gal}(L/K)^{ab}$ 中每个元素均映成单位元素. 根据 α, β, γ 的这些定义我们考虑下面的图表:

$$\begin{array}{ccccccc} & & A & & B & & \\ & & \downarrow & & \downarrow & & \\ 1 \rightarrow \text{Gal}(L/K)^{ab} & \xrightarrow{i} & U(L)/V(L/\bar{K}) & \xrightarrow{N} & U(K) & \rightarrow 1 & (3) \\ & \downarrow \gamma & \downarrow \alpha & & \downarrow \beta & & \\ 1 \rightarrow \text{Gal}(L/K)^{ab} & \xrightarrow{i} & U(\bar{L})/V(L/\bar{K}) & \xrightarrow{N} & U(K) & \rightarrow 1 & \\ & \downarrow & \downarrow & & & & \\ & C & D & & & & \end{array}$$

其中横行均是前述的 Galois 扩张 L/K 的基本正合序列(1). A 和 B 分别是 α 和 β 的核, C 和 D 分别是 γ 和 α 的余核.

引理 1 图表(3)是可交换的. 并且

$$\begin{aligned} A &= U(E)V(\bar{L}/\bar{K})/V(L/\bar{K}), \quad B = U(k_0), \\ C &= \text{Gal}(L/K)^{ab}, \quad D = 1. \end{aligned}$$

证明 从 $\phi|_{\bar{K}} = \varphi_0$ 即知 (3) 中右边的四边形是可交换的. 其次, 固定 L 的一个素元 π , 根据同态 i 的定义 (§2.2), $i(\sigma)$ ($\sigma \in \text{Gal}(L/K)$) 是 $U(\bar{L})/V(\bar{L}/\bar{K})$ 中包含 $\pi^{\sigma-1} = \sigma(\pi)/\pi$ 的剩余类. 由 §1.2, 引理 3 知道 $\pi^{\sigma-1} \in U(\bar{L})$, 从而

$$(\pi^{\sigma-1})^{\phi-1} = (\pi^{\phi-1})^{\sigma-1} \in V(L/\bar{K}).$$

于是 $\alpha \cdot i = 1$, 即 (3) 中左边的四边形也是交换的. 由 §4.2, 定理 2 知道 $\phi - 1: U(L) \rightarrow U(L)$ 的核是 $U(E)$, 从而由 (2) 式即知 $A = U(E)V(\bar{L}/\bar{K})/V(L/\bar{K})$. 再由 §4.2, 定理 2 即得 $B = U(k_0)$. 由 γ 的定义即知 $C = \text{Gal}(L/K)^{ab}$. 最后由 §4.2, 定理 2 还知道 $\phi - 1: U(L) \rightarrow U(\bar{L})$ 是满射; 从而 $D = 1$.

由于图表(3)是交换的, 映射 N 和 i 诱导出同态

$$A \rightarrow B, \quad C \rightarrow D.$$

将这两个同态加到图表(3)上, 它仍然是交换的. 为简单起见, 这个扩充了的图表今后也叫作图表(3).

由于(扩大了)图表(3)的两横行都是正合序列(1), 根据蛇形引理¹⁾, 存在同态 $\delta: B \rightarrow C$ 使得有正合序列

$$A \rightarrow B \rightarrow C \rightarrow D.$$

也就是说, 给了 $B = U(k_0)$ 中任意元素 v , 由图表的交换性和正合性, 可知存在元素 $\xi \in U(\bar{L})$, 使得 $v = N(\xi)$. 此外也存在元素 $\sigma \in C = \text{Gal}(L/K)^{ab}$, 使得 $i(\sigma) = \alpha(\xi \bmod V(\bar{L}/\bar{K}))$, 即 $\sigma(\bar{x})/\bar{x} \equiv \xi^{p^{-1}} \bmod V(\bar{L}/\bar{K})$. 由于 σ 由 v 所唯一决定, 令 $\delta(v) = \sigma$. 由此定义出映射 $\delta: B \rightarrow C$. 容易看出 δ 是同态, 并且 $A \rightarrow B \rightarrow C \rightarrow D$ 是正合序列.

由于在上面引理中 $D = 1$, 从而 $\delta: B \rightarrow C$ 是满射. 又由于 $\text{Ker} \delta = \text{Im}(A \rightarrow B)$, 因此

$$\begin{aligned} N(U(E))V(\bar{L}, \bar{K}) &= N_{E/k_0}(U(E)) \\ &= NU(E/k_0). \end{aligned}$$

于是 δ 诱导出一个基本同构映射

$$U(k_0)/NU(E/k_0) \cong \text{Gal}(L/K)^{ab}. \quad (4)$$

引理 2 Galois 群 $\text{Gal}(L/k)$ 自然地作用在图表(3)的每个群上, 则图表中的映射均是 $\text{Gal}(L/k)$ -模同态, 因此同构(4)也是 $\text{Gal}(L/k)$ -模同构.

证明 由于 K/k 是 Galois 扩张, 从而 $\text{Gal}(L/K)$ 是 $\text{Gal}(L/k)$ 的正规子群, 于是 $\text{Gal}(L/K)$ 的换位子群 $\text{Gal}(L/K)'$ 也是 $\text{Gal}(L/k)$ 的正规子群. 因此 $\text{Gal}(L/k)$ 的内自同构 $\tau \mapsto \rho\tau\rho^{-1}$ ($\tau \in \text{Gal}(L/k)$) 诱导出

$$\text{Gal}(L/K)^{ab} \rightarrow \text{Gal}(L/K)/\text{Gal}(L/K)'$$

的自同构, 由此给出 $\text{Gal}(L/k)$ 在 $\text{Gal}(L/K)^{ab}$ 上的自然作用. 设 $\rho \in \text{Gal}(L/k)$, 如果将 ρ 等同于 ρ 在 \bar{L} 上的扩充 $\bar{\rho}$, 则 ρ 显然将 $U(\bar{L})$ 映到自身之上. 对于 $\xi \in U(\bar{L})$, $\sigma \in \text{Gal}(L/K)$. 令 $\sigma' = \rho\sigma\rho^{-1}$, 则 $\sigma' \in \text{Gal}(L/K)$, 并且

1) 关于蛇形引理可参看代数学教科书, 例如 N. Bourbaki, *Algèbre commutative*, 第一章第 1 节. 事实上, 按照下面所叙述的图表追踪方法就可得到一般情形的证明.

$$\rho(\xi^{\sigma^{-1}}) = \rho(\sigma(\xi)/\xi) = \rho(\xi)^{\sigma'^{-1}},$$

从而 ρ 将 $U(L)$ 的子群 $V(\bar{L}/K)$ 映到自身之中. 由此给出 $\text{Gal}(L/k)$ 在 $U(\bar{L})/V(L/K)$ 上的自然作用. 由于 K/k 是 Galois 扩张, $\rho(K) = K$, 由此显然给出 $\text{Gal}(L/k)$ 在 $U(K)$ 上的作用. 设 π 是 \bar{L} 的素元, 与上面一样令 $\rho(\pi^{\sigma^{-1}}) = \rho(\pi)^{\sigma'^{-1}}$, 则

$$\begin{aligned}\rho(\iota(\sigma)) &= \iota(\rho\sigma\rho^{-1}), \quad \sigma \in \text{Gal}(L/K), \\ \rho &\in \text{Gal}(L'/k).\end{aligned}$$

从而映射 ι 是 $\text{Gal}(L/k)$ -模同态. 其次, 由于 $\text{Gal}(L/K)$ 是 $\text{Gal}(L/k)$ 的正规子群, 由此即知范映射 $N = N_{L/K}$ 是 $\text{Gal}(L/k)$ 上的同态, 前面已经证过 $\rho\psi = \psi\rho$. 同样也可知道 (或者利用 $\text{Gal}(K/k)$ 是 Abel 群这一事实) ρK 与 φ_0 也是可换的. 因此 α 和 β 是 $\text{Gal}(L/k)$ 模同态. 根据 γ 的定义显然 γ 也是 $\text{Gal}(L/k)$ 模同态. 最后, 不难看出, 由 N 和 ι 诱导的 $A \rightarrow B$ 和 $C \rightarrow D$ 也是 $\text{Gal}(L/k)$ 模同态. 从而图表 (3) 中的映射均是 $\text{Gal}(L/k)$ -模同态. 由此得到的 $\delta: B \rightarrow C$ 和同构 (4) 分别是 $\text{Gal}(L/k)$ -模同态和 $\text{Gal}(L/k)$ 模同构.

设 φ 是 K/k 的 Frobenius 自同构, 令

$$G = \text{Gal}(L/k), \quad H = \text{Gal}(L/K).$$

并且 φ 在 $G = \text{Gal}(L/k)$ 中的每个扩充仍记成 φ . 令 G_1 是由 H 和 φ 生成的 G 的子群. 由于 H 是 G 的正规子群, 从而 H 的换位子群 $H' = [H, H]$ 也是 G 的正规子群. 但是易知

$$H' \subseteq H^{\varphi^{-1}}H' \subseteq H.$$

从而 $H^{\varphi^{-1}}H'$ 是 G_1 的正规子群, 并且 $G_1/H^{\varphi^{-1}}H'$ 是 Abel 群. 由于 L/K 是有限扩张, H 是有限群, 因此 H 的子群 $H^{\varphi^{-1}}H'$ 对于 Krull 拓扑是 G 的闭子群. 另一方面, 由于 Frobenius 自同构 φ 生成 $G/H = \text{Gal}(K/k)$ 的稠子群, 从而 G_1 是 G 的稠子群. 因此 $H^{\varphi^{-1}}H'$ 也是 G 的正规子群, 并且 $G/H^{\varphi^{-1}}H'$ 是 Abel 群. 从而 $H^{\varphi^{-1}}H'$ 包含 G 的换位子群 $G' = [G, G]$: $G' \subseteq H^{\varphi^{-1}}H'$. 另一方面, 显然有 $H^{\varphi^{-1}}H' \subseteq G'$, 从而得到

$$G' = H^{\varphi^{-1}}H'.$$

特别地, G' 是 G 的闭子群. 根据 Galois 理论, $G' = H^{\varphi^{-1}}H'$ 所对应的中间域是 $k_{ab} \cap L$, 即是 L 中 k 的极大 Abel 扩域:

$$\text{Gal}(L/k_{ab} \cap L) = H^{\varphi^{-1}}H'.$$

由于 $\text{Gal}(L/k)^{ab} = H/H'$, 因此 $\text{Gal}(L/k)$ -模同构(4): $U(k_0)/NU(E/k_0) \cong H/H'$ 诱导出同构

$$\begin{aligned} U(k_0)/U(k_0)^{\varphi^{-1}}NU(E/k_0) &\cong H/H^{\varphi^{-1}}H' \\ &= \text{Gal}(k_{ab} \cap L/K). \end{aligned}$$

其次考虑范映射

$$N_{k_0/k}: U(k_0) \rightarrow U(k).$$

由于 k_0/k 是有限不分歧扩张, $\text{Gal}(k_0/k)$ 是由 $\varphi|_{k_0}$ 生成的循环群. 如果 $v \in N(k_0)$, $N_{k_0/k}(v) = 1$, 则由 Hilbert 定理可知存在 $z \in k_0^\times$ 使得 $v = z^{\varphi^{-1}}$. 由于 k 的素元 π 也是不分歧扩域 k_0 的素元, 从而 $z = \pi^m w$, $w \in U(k_0)$, $m \in \mathbb{Z}$. 于是 $v = w^{\varphi^{-1}}$, $w \in U(k_0)$. 所以上面同态 $N_{k_0/k}$ 的核是 $U(k_0)^{\varphi^{-1}}$. 利用 §3.3, 引理 4 可知 $N_{k_0/k}$ 诱导出

$$U(k_0)/U(k_0)^{\varphi^{-1}}NU(E/k_0) \cong U(k)/NU(E/k).$$

于是从早先证明的同构得出

$$U(k)/NU(E/k) \cong \text{Gal}(k_{ab} \cap L/K).$$

从以上诸结果得到下面的定理. 即: 设 E 是局部域 k 的任意有限 Galois 扩域, 而令

$$K = k_{ur}, k_0 = E \cap K, L = EK = E_{ur}, \bar{K}, \bar{L} \text{ 分别为}$$

$$K, L \text{ 的完备化, } \phi = L/E \text{ 的 Frobenius 自同构,}$$

$$\bar{\pi} \text{ 为 } \bar{L} \text{ 的素元,}$$

又记 $\text{Gal}(\bar{L}/\bar{K}) = \text{Gal}(L/K)$, 并以 $V(\bar{L}/\bar{K})$ 表示由 $\{\xi^{\sigma^{-1}} | \xi \in U(\bar{L}), \sigma \in \text{Gal}(\bar{L}/\bar{K})\}$ 生成的 $U(\bar{L})$ 的子群. 由于 $K \subseteq k_{ab} \cap L \subseteq L$, 以 $\sigma|_{k_{ab} \cap L}$ 表示元素 $\sigma \in \text{Gal}(L/K)$ 在 $k_{ab} \cap L$ 上的限制, 它是 $\text{Gal}(L/K)$ 的商群 $G(k_{ab} \cap L/K)$ 中的元素.

定理 1 设 E/k 是任意有限 Galois 扩张, 如上定义 $K, k_0, L = E_{ur}$ 等, 则对于 k 的单位群 $U(k)$ 中每个元素 u , 均存在元素 $v \in U(k_0)$, $\xi \in \bar{L}, \sigma \in \text{Gal}(\bar{L}/\bar{K})$, 使得

$$N_{k_0/k}(\nu) = u, N_{L/\bar{K}}(\xi) = v,$$

$$\bar{\pi}^{\sigma^{-1}} \equiv \xi^{\psi^{-1}} \pmod{V(\bar{L}/\bar{K})},$$

并且 $\sigma' k_{ab} \cap E_{ur}$ 只与 u 有关, 而映射

$$u \pmod{NU(E/k)} \mapsto \sigma' k_{ab} \cap E_{ur}$$

给出同构

$$\delta_{E/k}: U(k)/NU(E/k) \cong \text{Gal}(k_{ab} \cap E_{ur}/k_{ur}).$$

下面象 Hasse [6] 那样考查 E/k 是 Abel 扩张的情形, 这时 $L = E_{ur} = EK$ 是 k 的 Abel 扩张, 从而定理 1 中同构 $\delta_{E/k}$ 的右边为

$$\text{Gal}(L/K) = \text{Gal}(E/E \cap K) = \text{Gal}(E/k_0).$$

如果 E/k 是有限扩张, 令 $e = e(E/k)$, $f = f(E/k)$, 则由 §3.2, 定理 5 可知 $[E:k_0] = e$. 因此由同构 $\delta_{E/k}$ 给出

$$[U(k):NU(E/k)] = e. \quad (5)$$

这里的证明用到了定理 1 的结果, 但是等式(5)也可由引理 1 和蛇形引理直接按下述方法得到: 根据 §4.3, 引理 7, 令 E' 是 L/k 的补域, 即

$$E' \cap K = k, E'K = L,$$

则 E'/k 是有限 Galois 扩张. 对于 E'/k 定义与图表(3)一样的交换图表. 引理 1 和蛇形引理对于这个新图表也是适用的, 于是得到同构(代替(4)式):

$$U(k)/NU(E'/k) \cong \text{Gal}(L/K).$$

但是 $L = EK = E'K$, 从 §4.3 引理 5 有

$$NU(E'/k) = NU(L/k) = NU(E/k).$$

因此上面的同构也可写成 $U(k)/NU(E/k) \cong \text{Gal}(L/K)$. 然后即可与上面一样地得到(5)式.

令 v 是 k 的正规赋值, 由 §1.3, 定理 3 的系知道 $v(N(E/k)) = f\mathbb{Z}$, 再注意到 $N(E/k) \cap U(k) = NU(E/k)$, 从而利用 §1.3, 定理 3 即可由(5)式得出¹⁾

1) 参照下一章 §6.3, 定理 6 的证明.

$$\begin{aligned}
[k^{\times}: N(E/k)] &= [k^{\times}: N(E'/k)U(k)] \\
&\quad \cdot [N(E'/k)U(k): N(E'/k)] \\
&= [Z: Z \cap U(k): NU(E/k)] \\
&= j_e = [E:k].
\end{aligned}$$

从而对于任意有限 Abel 扩张 F/k 均有

$$[k^{\times}: N(E/k)] = [E:k].$$

这叫做局部类域论的基本等式。是局部类域论中最重要的结果之一。如此较为简单(而直接)地推导出基本等式,这是 Hazewinkel 方法的一个特色。本书以后在 §5.3 中将要使用稍微不同的方法给出基本等式的另外一个证明,甚至证明出同构 $k^{\times}/N(E/k) \cong \text{Gal}(E/k)$ 。但是为了阐明 Hazewinkel 思想的要点,我们还是介绍了以上的证明。

§5.2 $\delta_{E/k}$ 的性质

本节考查由二节定理 1 定义的同构 $\delta_{E/k}$ 的性质,特别是它与 Galois 扩张 E'/k 的依赖关系。以下令 $K = k_{ur}$, $k_0 = E \cap K$, $L = EK = E_{ur}$, 而 \bar{K} , \bar{L} , ϕ , π 等均如定理 1 所述。

设 E' 是 k 的有限 Galois 扩域并且包含在定理 1 的 E 之中: $k \subseteq E' \subseteq E$ 。显然有

$$\begin{aligned}
NU(E/k) &\subseteq NU(E'/k), \\
k_{ur} &\subseteq k_{ab} \cap E'_{ur} \subseteq k_{ab} \cap E_{ur},
\end{aligned}$$

于是可以定义自然同态

$$\begin{aligned}
U(k)/NU(E/k) &\rightarrow U(k)/NU(E'/k), \\
\text{Gal}(k_{ab} \cap E_{ur}/k_{ur}) &\rightarrow \text{Gal}(k_{ab} \cap E'_{ur}/k_{ur}).
\end{aligned}$$

将定理 1 用于 E'/k 则给出

$$\delta_{E'/k}: U(k)/NU(E'/k) \cong \text{Gal}(k_{ab} \cap E'_{ur}/k_{ur}).$$

引理 3 图表

$$U(k) : NU(E/k) \xrightarrow{\sim} \text{Gal}(k_{ab} \cap E_{ur}/k_{ur})$$

$$U(k) : NU(E'/k) \xrightarrow{\sim} \text{Gal}(k_{ab} \cap E'_{ur}/k_{ur})$$

是交换的.

证明 令 $k'_0 = E' \cap K$, $L = E'K = E'_{ur}$. 由定理 1 可知对于 $u \in U(k)$ 我们有

$$u = N_{k_0/k}(v), \quad v = N_{\bar{L}/\bar{K}}(\xi),$$

$$\bar{x}^{\sigma^{-1}} \equiv \xi^{\psi^{-1}} \pmod{V(\bar{L}'/\bar{K})},$$

$$v \in L(k_0), \quad \xi \in U(\bar{L}), \quad \sigma \in \text{Gal}(\bar{L}'/\bar{K}),$$

则引理中图表的上行是同构

$$u \pmod{NU(E/k)} \mapsto \sigma|_{k_{ab} \cap L}.$$

为简单起见令 $N = N_{L/L'}$, 则由 §2.2, (4) 式可知 $N(V(\bar{L}/\bar{K})) = V(\bar{L}'/\bar{K})$. 又由 §2.1, 引理 1 知道 \bar{L}'/\bar{L}' 完全分歧, 从而 $\pi' = N(\pi)$ 是 \bar{L}' 的素元. 另一方面, $\text{Gal}(L/L')$ 是 $\text{Gal}(L/k)$ 的正规子群, 从而 $N(\pi^{\sigma^{-1}}) = N(\pi)^{\sigma^{-1}} = \pi'^{\sigma^{-1}}$. 同样有 $N(\xi^{\psi^{-1}}) = N(\xi)^{\psi^{-1}}$. 若令 ϕ' 为 L'/E' 的 Frobenius 自同构, 又令

$$m = [k_0:k'_0] = [E \cap L':E'],$$

$$\omega = 1 + \phi' + \cdots + \phi'^{m-1},$$

则 $\phi|_{L'} = \phi'^m$. 其中 ϕ 是 L/E 的 Frobenius 自同构. 令 $\xi' = N(\xi)^\omega$, 于是 $N(\xi'^{-1}) = \xi'^{\psi^{-1}}$. 从而将关于 \bar{x} 和 ξ 的 $\pmod{V(\bar{L}'/\bar{K})}$ 同余式两边作用 $N = N_{L/L'}$, 即得

$$\bar{x}^{\sigma^{-1}} \equiv \xi'^{\psi^{-1}} \pmod{V(\bar{L}'/\bar{K})}.$$

由于 $\xi' = N(\xi)^\omega \in U(\bar{L}')$, 从而

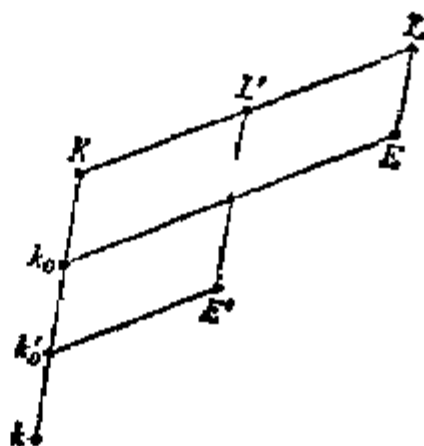
$$N_{L'/K}(\xi') = N_{L'/K}(N(\xi)^\omega)$$

$$= N_{L'/K}(\xi)^\omega = v^\omega.$$

将最后元素记成 v' . 由于 $\text{Gal}(k_0/k'_0)$ 是由 $\phi'|_{k_0}$ 生成的 m 阶循环群, 从而

$$v' = v^\omega = N_{k'_0/k_0}(v),$$

$$N_{k'_0/k}(v') = N_{k'_0/k}(v) = u.$$



且 $N_{E'/k}(\xi') = v' \in U(k_0)$, $N_{k_0/k}(v') = u$. 从而由定理 1 可知引理中图表下行的同构是

$$u \bmod NU(E'/k) \mapsto \sigma|_{k_{ab} \cap L'}.$$

并且也证明了图表是交换的.

引理 4 设 E 是 k 的任意有限 Galois 扩张, 则

$$\begin{aligned} NU(E'/k) &= NU(k_{ab} \cap E'/k) \\ &= NU(k_{ab} \cap E_{ur}/k). \end{aligned}$$

又如果 F 也是 k 的有限 Galois 扩张, 并且

$$k_{ab} \cap E_{ur} = k_{ab} \cap F_{ur},$$

则

$$\delta_{E/k} = \delta_{F/k}.$$

证明 由于 $k_{ur} \subseteq k_{ab} \cap E_{ur} \subseteq E_{ur} = k_{ur}E$, $\text{Gal}(E_{ur}/k_{ur}) \cong \text{Gal}(E/k_0)$. 因此若令

$$E' = (k_{ab} \cap E_{ur}) \cap E = k_{ab} \cap E,$$

则

$$E'_{ur} = k_{ur}E' = k_{ab} \cap E_{ur}.$$

一方面, 由于 $k_{ab} \cap E_{ur} = E'_{ur}$, 从而同构 $\delta_{E'/k}$ 和 $\delta_{E'/k}$ 有同样的象 $\text{Gal}(E'_{ur}/K)$. 于是由 $\delta_{E'/k}$ 和 $\delta_{E'/k}$ 给出有限群的同构

$$U(k)/NU(E'/k) \cong U(k)/NU(E'/k).$$

但是, $k \subseteq E' \subseteq E$, 从而 $NU(E'/k) \subseteq NU(E'/k)$, 因此

$$NU(E'/k) = NU(E'/k) = NU(k_{ab} \cap E'/k).$$

另一方面, 由 §4.3, 引理 5 即知

$$\begin{aligned} NU(k_{ab} \cap E_{ur}/k) &= NU(E'_{ur}/k) \\ &= NU(E'/k) = NU(E'/k). \end{aligned}$$

其次, 如果对于 F/k 满足 $k_{ab} \cap E_{ur} = k_{ab} \cap F_{ur}$, 则由上面证明结果可知 $NU(E'/k) = NU(F'/k)$, 于是同构 $\delta_{E'/k}, \delta_{F'/k}$ 的两边是同样的群. 再令 $E^* = EF$, 将引理 3 用于 $k \subseteq E \subseteq E^*$ 和 $k \subseteq F \subseteq E^*$, 可知 $\delta_{E'/k}$ 和 $\delta_{F'/k}$ 均是由 $\delta_{E^*/k}$ 诱导出来的映射, 从而 $\delta_{E'/k} = \delta_{F'/k}$.

设 k' 是 E/k 的中间域, 则 k'/k 未必是 Galois 扩张, 但

E/k 是有限 Galois 扩张, 从而定理 1 给出

$$\delta_{k',k}: U(k')/NU(E/k') \cong \text{Gal}(k'_{ab} \cap E_{ur}/k'_{ur}).$$

又显然 $N_{k',k}$ 定义出

$$U(k')/NU(E/k') \rightarrow U(k)/NU(E/k),$$

由于 $k \subset k'$, 从而

$$k_{ab} \subseteq k'_{ab}, \quad k_{ur} \subseteq k'_{ur}.$$

所以由限制映射定义出自然同态

$$\text{Gal}(k'_{ab} \cap E_{ur}/k'_{ur}) \rightarrow \text{Gal}(k_{ab} \cap E_{ur}/k_{ur}).$$

引理 5 图表

$$U(k')/NU(E/k') \cong \text{Gal}(k'_{ab} \cap E_{ur}/k'_{ur})$$

↓

$$U(k)/NU(E/k) \cong \text{Gal}(k_{ab} \cap E_{ur}/k_{ur})$$

是交换的.

证明 令 $k' = k' \cap K$, $M = k'K \cap k'_{ur}$, $k_0 = E \cap M$. 对于元素 $u \in U(k')$ 令

$$u' = N_{k'_0/k'}(v'), \quad v' = N_{\bar{L}/\bar{M}}(\xi),$$

$$\bar{\pi}^{\sigma^{-1}} = \xi^{\sigma^{-1}} \bmod V(\bar{L}/\bar{M}),$$

$$v' \in U(k'_0), \quad \xi \in \bar{L}, \quad \sigma \in \text{Gal}(L/M),$$

则定理 1 给出引理中图表上行的同

态是

$$u \bmod NU(E/k') \mapsto$$

$$\sigma|_{k_{ab} \cap L}.$$

令

$$u = N_{k'_0/k}(u'),$$

$$v = N_{k'_0/k_0}(v'),$$

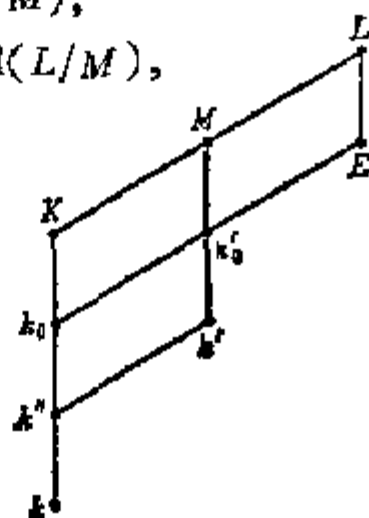
则

$$u = N_{k'_0/k}(v') = N_{k'_0/k}(v),$$

$$v = N_{\bar{M}/\bar{K}}(v') = N_{\bar{L}/\bar{K}}(\xi).$$

又由定义知道 $V(\bar{L}/\bar{M}) \subseteq V(L/\bar{K})$, 从而

$$\bar{\pi}^{\sigma^{-1}} = \xi^{\sigma^{-1}} \bmod V(L/\bar{K}).$$



因此由定理 1 给出引理中图表下行的同构是

$$u \bmod NU(E/k) \mapsto \sigma|_{k_{ab} \cap L}.$$

从而可知这个图表是交换的.

为了叙述下面的引理,还需要作一些群论上的准备,我们先作些简单的说明. 设 G 是任意的群, H 是 G 的子群并且指数 $[G:H]$ 有限, $G' = [G, G]$, $H' = [H, H]$ 分别是 G 和 H 的换位子群, 又令 $\{\sigma_1, \dots, \sigma_n\}$ 是 G 对于 H 的左陪集代表元系, 即

$$G = \bigcup_{i=1}^n H\sigma_i, \quad n = [G:H].$$

固定 G 中一个元素 σ , 则

$$H\sigma_i \mapsto H\sigma_i\sigma \quad (1 \leq i \leq n)$$

定义出陪集集合 $\{H\sigma_i | 1 \leq i \leq n\}$ 上的一个置换. 从而对于每个 i , 满足

$$\sigma_i\sigma = h_i\sigma_{i'}$$

的元素 $h_i \in H$ 和下标 i' ($1 \leq i' \leq n$) 是唯一决定的. h_i 作为 σ 的函数写成 $h_i(\sigma)$, 然后定义 $H^{ab} = H/H'$ 中元素

$$t_{G/H}(\sigma) = \prod_{i=1}^n h_i(\sigma)H'.$$

$t_{G/H}(\sigma)$ 与代表元系 $\{\sigma_1, \dots, \sigma_n\}$ 的选取无关而只依赖于 σ , 并且可以证明 $\sigma \mapsto t_{G/H}(\sigma)$ 是同态¹⁾

$$t_{G/H}: G \rightarrow H^{ab}.$$

由于 H^{ab} 是 Abel 群, 因此上面的 $t_{G/H}$ 诱导出从 $G^{ab} = G/G'$ 到 $H^{ab} = H/H'$ 的同态, 为简单起见这个诱导出来的同态仍记为

$t_{G/H}$:

$$t_{G/H}: G^{ab} \rightarrow H^{ab}.$$

并且将 $t_{G/H}$ 叫作从 G 到它的子群 H , 或者叫作从 G^{ab} 到 H^{ab} 的转移 (transfer). 若 U 是 H 的子群并且指数 $[H:U]$ 有限, 则又可

1) 这一结果以及随后所叙述的关于 $t_{G/H}$ 的性质均可由定义比较简单地直接推导出来. 详见群论教科书, 例如 M. Hall, The theory of groups, 第十四章 §2.

象上面那样定义

$$t_{G/U}: G^{ab} \rightarrow U^{ab}, \quad t_{H/U}: H^{ab} \rightarrow U^{ab},$$

并且有

$$t_{G/U} = t_{H/U} \circ t_{G/H}. \quad (6)$$

又设 N 是 G 的正规子群, 利用 $t_{G/H} = t_{HN/H} \circ t_{G/HN}$ 不难看出, $t_{G/H}: G^{ab} \rightarrow H^{ab}$ 将 NG'/G' 映到 $(H \cap N)H'/H'$ 之中:

$$NG'/G' \rightarrow (H \cap N)H'/H'.$$

注记 设群 G 在有理整数加法群 \mathbf{Z} 上的作用是平凡的, 则 $G^{ab} = H_1(G, \mathbf{Z})$, 并且转移映射 $t_{G/H}: G^{ab} \rightarrow H^{ab}$ 恰好是上司调群的限制映射¹⁾

$$H_1(G, \mathbf{Z}) \rightarrow H_1(H, \mathbf{Z}).$$

今后在应用时, G 是紧群(特别是射影有限群), H 是 G 的开子群. 这时令 $G' = [G, G]$ 和 $H' = [H, H]$ 分别代表 G 和 H 的拓扑换位子群, 即代数定义的换位子群在 G 中的闭包. 与上面一样的定义紧群的转移 $t_{G/H}: G \rightarrow H^{ab}$ 和 $t_{G/H}: G^{ab} \rightarrow H^{ab}$, 则 $t_{G/H}$ 是连续同态.

对于局部域 k , 令 \mathcal{O}_k 是包含在代数闭包 $\bar{\mathcal{O}}$ 中的 k 之极大可分扩域. 由于 \mathcal{O}_k/k 是 Galois 扩张, 从而 \mathcal{O}_k 也是 k 的极大 Galois 扩域. 设 k' 为 k 的任意有限可分扩域, $n = [k':k]$, 则

$$k \subseteq k' \subseteq \mathcal{O}_k.$$

如果令

$$G = \text{Gal}(\mathcal{O}_k/k), \quad H = \text{Gal}(\mathcal{O}_k/k'),$$

则 H 是 G 的闭子群并且指数 $[G:H]$ 有限, 从而 H 也是 G 的开子群:

$$H \subseteq G, \quad [G:H] = [k':k] = n.$$

根据拓扑换位子群 $G' = [G, G]$, $H' = [H, H]$ 以及 $G^{ab} = G/G'$ 和 $H^{ab} = H/H'$ 的定义, 可知

$$G^{ab} = \text{Gal}(k_{ab}/k), \quad H^{ab} = \text{Gal}(k'_{ab}/k').$$

1) 参见 Serre [11], 第七章 §8. 利用这一结果立刻得到前面所说的关于转移映射的一些性质(例如(6))

从而上述的转移 $\iota_{G/H}$ 定义出从 $\text{Gal}(k_{ab}/k)$ 到 $\text{Gal}(k'_{ab}/k')$ 的同态. 以后将这个同态写成 $\iota_{k'/k}$, 并且叫作从 k 到 k' 的 Galois 群的转移:

$$\iota_{k'/k}: \text{Gal}(k_{ab}/k) \rightarrow \text{Gal}(k'_{ab}/k').$$

给了元素 $\sigma \in \text{Gal}(k_{ab}/k)$, 计算 $\iota_{k'/k}(\sigma)$ 的方法如下: 首先将 σ 扩充成 Ω 的一个 k -自同构, 并且将如此得到的 $G = \text{Gal}(\Omega/k)$ 中元素仍记成 σ . 其次选取 G 对于 H 的一组左陪集代表元系 $\{\sigma_1, \dots, \sigma_n\}$, 然后如上定义 $h_i(\sigma) (1 \leq i \leq n)$, 再令

$$h(\sigma) = \prod_{i=1}^n h_i(\sigma),$$

最后令 $\iota_{k'/k}(\sigma) = h(\sigma)H'$, 即

$$\iota_{k'/k}(\sigma) = h(\sigma)|_{k'_{ab}}.$$

如果 k'' 是 k' 的任意有限可分扩域, 定义

$$\iota_{k''/k'}: \text{Gal}(k'_{ab}/k') \rightarrow \text{Gal}(k''_{ab}/k''),$$

$$\iota_{k''/k}: \text{Gal}(k_{ab}/k) \rightarrow \text{Gal}(k''_{ab}/k'').$$

则由(6)式立即得到

$$\iota_{k''/k} = \iota_{k''/k'} \circ \iota_{k'/k}.$$

引理 6 设 k'/k 是有限可分扩张, 则转移 $\iota_{k'/k}: \text{Gal}(k_{ab}/k) \rightarrow \text{Gal}(k'_{ab}/k')$ 诱导出子群之间的同态

$$\text{Gal}(k_{ab}/k_{ur}) \rightarrow \text{Gal}(k'_{ab}/k'_{ur}).$$

又若 E 是包含 k' 的 k -有限 Galois 扩域, 则 $\iota_{k'/k}$ 也诱导出同态

$$\text{Gal}(k_{ab} \cap E_{ur}/k_{ur}) \rightarrow \text{Gal}(k'_{ab} \cap E_{ur}/k'_{ur}).$$

证明 令 $T = \text{Gal}(\Omega/k_{ur})$, $N = \text{Gal}(\Omega/E)$, 则 T 和 N 均是 $G = \text{Gal}(\Omega/k)$ 的闭正规子群, 已经说过 $\iota_{k'/k} = \iota_{G/H}$ 是映射

$$TG'/G' \rightarrow (T \cap H)H'/H',$$

$$(T \cap N)G'/G' \rightarrow (T \cap N \cap H)H'/H',$$

由此诱导出

$$TG'/(T \cap N)G' \rightarrow (T \cap H)H'/(T \cap N \cap H)H'.$$

因为 $H' \subseteq G' \subseteq T \subseteq G$, $N \subseteq H$, 所以

$$\begin{aligned}TG' &= T, (T \cap H)H' = T \cap H, \\(T \cap N \cap H)H' &= (T \cap N)H'.\end{aligned}$$

注意 $k'_{ur} = k'k_{ur}$, $E_{ur} = Ek_{ur}$, $T \cap H = \text{Gal}(\mathcal{Q}_s/k'_{ur})$, $T \cap N = \text{Gal}(\mathcal{Q}_s/E_{ur})$, 从而上面的映射就是引理中所述的 Galois 群之间的同态.

如上令 k', k 是有限可分扩张, E 是包含 k' 的 k 之有限 Galois 扩张. 由 $\mathcal{L}(k) \subseteq \mathcal{L}(k')$ 给出的自然单射 $U(k) \rightarrow U(k')$ 将 $NU(E/k)$ 映到 $NU(E/k')$ 之中, 因此可定义同态

$$U(k)/NU(E/k) \rightarrow U(k')/NU(E/k').$$

引理 7 图表

$$\begin{array}{ccc}U(k)/NU(E/k) & \xrightarrow{\sim} & \text{Gal}(k_{ab} \cap E_{ur}/k_{ur}) \\ \downarrow & & \downarrow \\ U(k')/NU(E/k') & \xrightarrow{\sim} & \text{Gal}(k'_{ab} \cap E_{ur}/k'_{ur})\end{array}$$

是交换的. 其中右边竖线是引理 6 中由转移 $i_{k'}/k$ 诱导出来的同态, 而两个横向同构分别是 $\delta_{E/k}$ 和 $\delta_{E/k'}$.

证明 象引理 5 的证明中那样令 $k' = k' \cap K$, $M = kK = k'_{ur}$, $k_0 = E \cap M$. 对于任意元素 $u \in U(k)$, 令

$$\begin{aligned}u &= N_{k_0/k}(v), \quad v = N_{L/K}(\xi), \\ \pi^{\sigma^{-1}} &= \xi^{\sigma^{-1}} \bmod V(\bar{L}/\bar{K}), \quad v \in U(k_0), \\ \xi &\in U(\bar{L}), \quad \sigma \in \text{Gal}(L/K),\end{aligned}$$

则由定理 1 知道引理中图表上行的映射是

$$u \bmod NU(E/k) \mapsto \sigma|_{k_{ab} \cap E_{ur}}.$$

K/k 的 Frobenius 自同构 φ 到 $G = \text{Gal}(\mathcal{Q}_s/k)$ 的任意一个扩充仍记为 φ , 又令

$$\begin{aligned}v' &= v^{\omega}, \quad \omega = 1 + \varphi + \cdots + \varphi^{l-1}, \\ l &= [k'':k],\end{aligned}$$

则(参见引理 5 的证明中的图表)

$$N_{k_0'/k'}(v') = N_{k_0'/k''}(v') = N_{k_0/k}(v) = u.$$

又由于 $\text{Gal}(L/K)$ 是 $\text{Gal}(L/k)$ 的正规子群, 从而由 $v = N_{L/K}(\xi)$ 可知

$$\nu' = N_{\Gamma/K}(\xi^a).$$

又由于 $k' \cap K = k''$, $k'K = M$, 可知 $\text{Gal}(\mathcal{Q}_i/K)$ 对于 $\text{Gal}(\mathcal{Q}_i/M)$ 的左陪集代表元系 $\{\tau_1, \dots, \tau_m\}$ ($m = [M:K] = [k':k'']$) 同时也是 $\text{Gal}(\mathcal{Q}_i/k'')$ 对于 $\text{Gal}(\mathcal{Q}_i/k')$ 的左陪集代表元系. 因此

$$\{\sigma_1, \dots, \sigma_n\} = \{\tau_a \varphi^b \mid 1 \leq a \leq m, \\ 0 \leq b \leq l-1\}$$

是 $G = \text{Gal}(\mathcal{Q}_i/k)$ 对于 $H = \text{Gal}(\mathcal{Q}_i/k')$ 的左陪集代表元系. 从而

$$\nu' = N_{\bar{L}/M} \left(\prod_{i=1}^m \tau_i(\xi^a) \right) = N_{\bar{L}/M} \left(\prod_{i=1}^m \sigma_i(\xi) \right),$$

由此得到

$$\nu' = N_{\bar{L}/M}(\xi'), \quad \xi' = \prod_{i=1}^n \sigma_i(\xi) \in U(\bar{L}).$$

另一方面, 令

$$\pi^{\sigma^{-1}} = \xi^{\psi^{-1}} \eta, \quad \eta \in V(\bar{L}/\bar{K}),$$

在引理 2 的证明中已经说过, L/E 的 Frobenius 自同构 ψ 属于 $\text{Gal}(L/k)$ 的中心, 从而由 ξ' 的定义可知

$$\prod_{i=1}^n \sigma_i(\pi^{\sigma^{-1}}) = \xi'^{\psi^{-1}} \prod_{i=1}^n \sigma_i(\eta). \quad (7)$$

我们将元素 $\tau \in \text{Gal}(L/K)$ 到 $\text{Gal}(\mathcal{Q}_i/K)$ 中的扩充仍记成 τ , 并且象过去那样令

$$\sigma_i \tau = h_i(\tau) \sigma_{i'},$$

则对于任意元素 $0 \neq \alpha \in \bar{L}$, 我们有

$$\begin{aligned} \prod_{i=1}^n \sigma_i(\alpha^{\tau^{-1}}) &= \prod_{i=1}^n \sigma_i \tau(\alpha) \prod_{i=1}^n \sigma_{i'}(\alpha)^{-1} \\ &= \prod_{i=1}^n \sigma_{i'}(\alpha)^{h_i(\tau)-1}. \end{aligned}$$

但是 $\text{Gal}(\mathcal{Q}_s/K)$ 是 $\text{Gal}(\mathcal{Q}_s/k)$ 的正规子群, 令 $\sigma_i = \tau_a \varphi^b$, 则

$$\begin{aligned}\sigma_i \tau &= \tau_a \varphi^b \tau = \tau_a \tau' \varphi^b, \quad \tau' = \varphi^b \tau \varphi^{-b} \in \text{Gal}(\mathcal{Q}_s/K), \\ &= \tau'' \tau_a \varphi^b, \quad \tau'' \in \text{Gal}(\mathcal{Q}_s/M).\end{aligned}$$

从而 $\sigma_{i'} = \tau_a \varphi^b$. 又由于 $h_i(\tau) = \tau'' \in \text{Gal}(\mathcal{Q}_s/M)$, 从而 $h_i(\tau) | L \in \text{Gal}(L/M)$. 因此当 $\alpha \in U(\bar{L})$ 时, 由上式可知

$$\prod_{i=1}^n \sigma_i(\alpha^{\tau^{-1}}) \in V(\bar{L}/M).$$

但是上面的 $\eta \in V(\bar{L}/K)$ 是这样的 $\alpha^{\tau^{-1}}$ 之乘积, 从而

$$\prod_{i=1}^n \sigma(\eta) \in V(\bar{L}/\bar{M}).$$

其次, 将以上的注记用于 $\tau = \sigma$, $\alpha = \bar{\pi}$, 利用 §2.2, 引理 4 便得到

$$\begin{aligned}\prod_{i=1}^n \sigma_i(\bar{\pi}^{\sigma^{-1}}) &= \prod_{i=1}^n \sigma_{i'}(\bar{\pi})^{h_i(\sigma)-1} \\ &= \bar{\pi}^{h(\sigma)-1} \bmod V(\bar{L}/\bar{M}).\end{aligned}$$

其中 $h(\sigma) = \sum_{i=1}^n h_i(\sigma)$. 因此由(7)式即知

$$\bar{\pi}^{h(\sigma)-1} = \xi'^{\psi^{-1}} \bmod V(\bar{L}/\bar{M}).$$

由于 $u = N_{k'_{ab}/k'}(v')$, $v' = N_{L/\bar{M}}(\xi')$, 从而由定理 1 可知引理中图表下行的同构为

$$u \bmod NU(E/k') \mapsto h(\sigma) | k'_{ab} \cap E_{ur},$$

但是 $h(\sigma) | k'_{ab} = t_{k'/k}(\sigma)$, 这就证明了引理.

§ 5.3 拓扑同构 δ_k

继续设 $K = k_{ur}$, 我们考查满足如下条件的 k_{ab}/k 的中间域 M

$$k \subseteq K \subseteq M \subseteq k_{ab}, \quad [M:K] < +\infty. \quad (8)$$

对于任意有限 Galois 扩张 E/k , 令

$$M_E = k_{ab} \cap E_{nr},$$

则 M_E 显然满足条件(8). 另一方面, 对于每个满足(8)式的 M , 必然存在有限 Galois 扩张 E/k , 使得

$$M = M_E.$$

事实上, 由 §4.3, 引理 7 知道 M/k 具有补域 $E(=k')$. 由于 E/k 是有限 Galois 扩张并且 $M = E_{nr}$, 从而 $M_E = k_{ab} \cap E_{nr} = M$. 虽然 E 不是由 M 所唯一决定的, 但是如果 $M = M_E = M_F$, 则由引理 4 知道 $\delta_{E/k} = \delta_{F/k}$, 从而 $\delta_{E/k}$ 依赖于 M . 对于满足 $M = M_E$ 的 E , 今后将 $\delta_{E/k}$ 写成 $\delta_{M/k}$. 由引理 4 知道 $NU(E/k) = NU(M_E/k)$, 从而有同构

$$\delta_{M/k}: U(k)/NU(M/k) \xrightarrow{\sim} \text{Gal}(M/K).$$

如果 $K \subseteq M' \subseteq M$ 并且 M' 也满足(8)式, 定义

$$\delta_{M'/k}: U(k)/NU(M'/k) \xrightarrow{\sim} \text{Gal}(M'/K),$$

由引理 3 (和上面的注记) 知道图表

$$\begin{array}{ccc} U(k)/NU(M/k) & \xrightarrow{\sim} & \text{Gal}(M/K) \\ \downarrow & & \downarrow \\ U(k)/NU(M'/k) & \xrightarrow{\sim} & \text{Gal}(M'/K) \end{array} \quad (9)$$

是交换的. 由于两竖线映射的核分别是 $NU(M'/k)/NU(M/k)$ 和 $\text{Gal}(M/M')$, 由此可知 $\delta_{M/k}$ 诱导出子群同构

$$NU(M'/k)/NU(M/k) \xrightarrow{\sim} \text{Gal}(M/M').$$

因此可以证明关于单位范群的如下结果:

引理 8 设 k' 是 k 的有限 Abel 扩域, 则

$$U(k)/NU(k'/k) \simeq \text{Gal}(k'/k \cap k_{nr}),$$

$$[U(k):NU(k'/k)] = [k':k' \cap k_{nr}].$$

又如果 k' 是 k/k 的中间域 k_1, \dots, k_n 的合成域, 则

$$NU(k'/k) = \bigcap_{i=1}^n NU(k_i/k).$$

证明 令 $M = k \wedge$, 则 M 满足上述条件(8) 并且 $\text{Gal}(M/K) \simeq \text{Gal}(k'/k' \cap K)$. 由此可知 $\delta_{M/k}$ 给出同构 $U(k)/NU(M/k)$

$\cong \text{Gal}(k'/k \cap K)$. 再由引理 4 知道 $NU(M/k) = NU(k'/k)$, 从而证明了引理的前一半.

其次令 $M_i = k_i K$, 则 M 是 M/K 的中间域 $M_i (1 \leq i \leq n)$ 的合成域. 因此 $\text{Gal}(M/M_i) (1 \leq i \leq n)$ 的公共元素只有 1. 由上面的注记知道同构 $\delta_{M/k}$ 将 $NU(k/k)/NU(k'/k)$ 映到 $\text{Gal}(M/M_i)$ 之上, 从而得到引理的后一半.

注记 也可以用定理 1 后面的等式 (5) 以稍微不同的方法证明此引理的前一半.

k 的极大 Abel 扩域 k_{ab} 显然是满足 (8) 式的全部中间域 M 之并集合. 从 § 4.1 的注记知道

$$\text{Gal}(k_{ab}/K) = \varprojlim \text{Gal}(M'/K).$$

其中右边关于 M 的射影极限是对于 $K \subseteq M' \subseteq M$ 的自然同态 $\text{Gal}(M'/K) \rightarrow \text{Gal}(M'/K)$ 所定义的. 另一方面, 由单位范群的定义可知

$$\bigcap_M NU(M/k) = NU(k_{ab}/k),$$

同样地对于 M 作射影极限, 便得到

$$U(k)/NU(k_{ab}/k) = \varprojlim U(k)/NU(M/k).$$

使用交换图表 (9), 然后对于由 M 定义的有限群的同构 $\delta_{M/k}$ 作射影极限, 即定义出紧群同构

$$\delta_k: U(k)/NU(k_{ab}/k) \xrightarrow{\sim} \text{Gal}(k_{ab}/k_{nr}).$$

由于 k_{ab} 是集族 $\{M_E = k_{ab} \cap E_{nr} \mid E/k \text{ 为有限 Galois 扩张}\}$ 的并集, 对于 E 同样作射影极限, 即得到

$$\text{Gal}(k_{ab}/K) = \varprojlim \text{Gal}(M_E/K).$$

又由

$$\bigcap_E NU(E/k) = NU(\mathcal{Q}_r/k),$$

显然得到

$$U(k)/NU(\mathcal{Q}_r/k) = \varprojlim U(k)/NU(E/k).$$

再由引理 3 即知由所有对 E/k 定义的同构 $\delta_{E/k}$ 得到

$$U(k)/NU(\mathcal{O}_s/k) \xrightarrow{\sim} \text{Gal}(k_{ab}/k_{s^*}),$$

并且当 $M = M_E$ 时, 则 $\delta_{M/k} = \delta_{E/k}$. 因此, 上面定义的同构与 δ_k 一致. 特别地得到

$$NU(k_{ab}/k) = NU(\mathcal{O}_s/k).$$

(这也可以用引理 4 直接得出.) 其次, 由于上面单位范群均包含 1, 这样我们就分成几步证明了 δ_k 是同构映射.

下面对于局部域 k 使用第二章中的记号和结果. 令 q 为 k 的剩余类域 $\mathbb{F} = \mathcal{O}_k/\mathfrak{p}$ 的元素个数, $U = U_0 = U(k)$, $U_n = 1 + \mathfrak{p}^n$ ($n \geq 1$). 由 §3.1, 定理 3 知道 U 包含 $q-1$ 阶循环群 V , 并且

$$U = V \times U_1.$$

于是 k 包含 $(q-1)$ 次本原单位根, 设 π' 是 k 的素元 π 的 $(q-1)$ 次根, 并且令

$$k' = k(\pi'), \quad \pi'^{q-1} = \pi,$$

则 k'/k 是循环扩张并且次数 $n = [k':k]$ 不超过 $q-1$; $n \leq q-1$. 设 v 和 v' 分别是 k 和 k' 的正规赋值, 而令 $e = e(k'/k)$, $f = f(k'/k)$, 则由 §1.3 可知 $v'k = ev$, 再由定理 3 即知

$$ef = n \leq q-1 \leq (q-1)v'(\pi')$$

$$v'(\pi') = ev(\pi) = e.$$

因此 $n = q-1 = e$, 即 k'/k 是 $(q-1)$ 次完全分歧循环扩张. (注意 $X^{q-1} - \pi \in k[X]$ 是 Eisenstein 多项式, 从而这一点也可由 Eisenstein 多项式的一般理论得出.) 再由引理 8 可知

$$[U(k):NU(k'/k)] = q-1.$$

特别地, $NU(k'/k)$ 是 $U = U(k)$ 的开子群, 从而由 §3.1 的定理 3 可知, 对于充分大的 $i \geq 1$, 我们有

$$U_i \subseteq NU(k'/k) \subseteq U, \quad [U:U_i] = (q-1)q^{i-1}.$$

由于 $q-1 = [U:U_1]$ 与 $q^{i-1} = [U_i:U_1]$ 互素, 从而

$$NU(k'/k) = U_1,$$

于是得到

$$NU(\mathcal{O}_s/k) = NU(k_{ab}/k) \subseteq U_1.$$

引理 9 设 k 是 p 局部域, 则

$$NL(Q/k) \subset U^p.$$

证明 先考虑 k 的特征为 0 的情形. 设 ζ 是 Q 中的 p 次本原单位根, $k' = k(\zeta)$, 则由 §3.1, 引理 2 知道 $k'^{\times}/(k'^{\times})^p$ 和 $U(k')/U(k')^p$ 均是有限群. 如果 $U(k')/U(k')^p$ 作为 (p, p, \dots, p) 型 Abel 群的秩是 m , 则 $k'^{\times}/(k'^{\times})^p$ 是秩为 $m+1$ 的 (p, \dots, p) 型 Abel 群. 以 k'' 表示将 k' 中全部元素的 p 次根添加到 k' 上而得到的域. 由于 $\zeta \in k'$, 从而 k''/k' 是 Kummer 扩张, 从而 $\text{Gal}(k''/k')$ 与 $k'^{\times}/(k'^{\times})^p$ 同构 (但不是标准的同构). 由于 k'' 是 k' 的全部 p 次循环扩张之合成域, 利用 §3.2, 定理 4 即知 $k'' \cap k_{ur}$ 是 k' 的 p 次不分歧扩张, 于是 $\text{Gal}(k''/k'' \cap k_{ur})$ 是秩 m 的 (p, \dots, p) 型 Abel 群. 再由引理 8 可知 $U(k')/NU(k''/k')$ 也是秩 m 的 (p, \dots, p) 型 Abel 群, 特别地得到 $U(k')^p \subseteq NU(k''/k')$. 但是 $U(k')/U(k')^p$ 的秩是 m , 因此

$$NU(k''/k') = U(k')^p.$$

将等式两边作用 $N_{k'/k}$, 由于 $k \subset k' \subseteq Q$, 从而得到

$$\begin{aligned} NU(Q/k) &\subset NU(k''/k) \\ &= NU(k'/k)^p \subseteq U(k)^p = U^p. \end{aligned}$$

其次设 k 的特征为 p , 这时可以利用 §3.3, 引理 6 以及在它前面所叙述的结果. 象那里那样定义 k 的加法群 k^+ 的自同态 $r: k^+ \rightarrow k^+$ 以及 k^+ 的子群 $A_n, B_n (n \geq 0)$. 并且对于任意元素 $x \in k$, 用 k_x 表示 k 的扩张 $k(\alpha)$, 其中 α 是 Q 中满足 $\alpha^p - \alpha = x$ 的元素. 由于 $[A_n : B_n] < +\infty$, 对于固定的 $n \geq 1$, 以 k' 表示 $\{k_x, x \in A_n\}$ 的合成域, 由 Artin-Schreier 理论可知 k'/k 是 Abel 扩张, 从而 $\text{Gal}(k'/k)$ 同构于 A_n/B_n , 并且

$$[k':k] \cdot [A_n : B_n] = pq^{n-m}, m = \left[\frac{n}{p} \right].$$

如果 $x \in F, x \notin r(F)$, 则 k_x/k 为 p 次不分歧扩张, 由上述同构可知 $\text{Gal}(k'/k)$ 是 (p, p, \dots, p) 型 Abel 群并且 $[k' \cap k_{ur} : k] = p$, 从而 $\text{Gal}(k'/k' \cap k_{ur})$ 是型为 (p, p, \dots, p) 的 q^{n-m} 阶 Abel

群. 于是由引理 8 可得

$$U^p \subseteq NU(k'/k) \subseteq U, [U:NU(k'/k)] = q^{n-m}.$$

另一方面, 由 §3.3, 引理 6 可知对于每个 $x \in A_n$ 均有

$$U_{n+1} \subseteq NU(k_x/k),$$

从而由引理 8 有 $U_{n+1} \subseteq NU(k'/k)$, 再与上面的包含关系合在一起, 即得上

$$U^p U_{n+1} \subseteq NU(k'/k) \subseteq U.$$

此外, 在 §3.3 中已经得到

$$[U:U^p U_{n+1}] = q^{n-m},$$

从而由上述可知

$$NU(k'/k) = U^p U_{n+1} \quad (n \geq 1).$$

于是

$$NU(\mathcal{Q}_i/k) = NU(k_{\infty}/k) \subseteq \bigcap_{n \geq 1} U^p U_n.$$

根据 §3.1, 定理 3, $\{U_n\}_{n \geq 1}$ 形成 1 在 k^\times 中的基本邻域系, 因此上式右边的交集是 U^p 在 k^\times 中的闭包. 由于 U^p 是紧群 U 在 $x \mapsto x^p$ 之下的连续象, 从而也是紧群, 于是

$$U^p = \bigcap_{n \geq 1} U^p U_n.$$

所以在这种场合, $NU(\mathcal{Q}_i/k)$ 也包含在 U^p 之中, 从而证明了引理.

定理 2 $N(k_{\infty}/k) = NU(k_{\infty}/k) = 1$.

证明 设 k 是 p 局部域, k' 是 k 的任意有限可分扩域, 由上述引理可知

$$NU(\mathcal{Q}_i/k') \subseteq U(k')^p.$$

两边作用 $N_{k'/k}$, 再由 §4.1, 引理 2, 可知

$$NU(\mathcal{Q}_i/k) \subseteq NU(k'/k)^p.$$

从而用 §4.1, 引理 1 得到 $NU(\mathcal{Q}_i/k) \subseteq NU(\mathcal{Q}_i/k)^p$, 于是

$$NU(\mathcal{Q}_i/k) = NU(\mathcal{Q}_i/k)^p.$$

从而对每个 $m \geq 1$ 均有

$$NU(\mathcal{Q}_i/k) = NU(\mathcal{Q}_i/k)^{p^m}.$$

但是已经证明了 $NU(\mathcal{Q}_i/k) \subseteq U_1$, 从而 $[U_1:U_n] = q^{n-1}$ 是 p 的幂, 于是对于每个 $n \geq 1$ 均有

$$NU(\mathcal{Q}_i/k) \subseteq U_n.$$

从而

$$NU(k_{ab}/k) = NU(\mathcal{Q}/k) = 1.$$

进而, 由 §4.3, 引理 3 知道

$$N(k_{ab}/k) \subseteq N(k_{ur}/k) \cap U(k),$$

利用 §4.1 中所作的一般性注记即知

$$\begin{aligned} N(k_{ab}/k) &= N(k_{ab}/k) \cap U(k) \\ &= NU(k_{ab}/k) = 1. \end{aligned}$$

作为说明, 由定理 2 得到如下的结果:

定理 3 对于每个有限 Galois 扩张 E/k 均由定理 1 定义出同构 $\delta_{E/k}$, 又对于满足条件(8)的每个域 M 定义同构 $\delta_{M/k}$, 取极限之后即可定义出射影有限群之间的拓扑同构

$$\delta_k: U(k) \xrightarrow{\sim} \text{Gal}(k_{ab}/k_{ur}).$$

下面两个结果涉及到 δ_k 与 k 的依赖关系, 它们均可由上节的引理很容易地推导出来.

定理 4 设 k' 是 k 的任意有限可分扩张, 则图表

$$\begin{array}{ccc} U(k') & \xrightarrow{\sim} & \text{Gal}(k'_{ab}/k'_{ur}) \\ \downarrow & & \downarrow \\ U(k) & \xrightarrow{\sim} & \text{Gal}(k_{ab}/k_{ur}) \end{array}$$

是交换的. 其中左边竖线为范映射 $N_{k'/k}$, 右边竖线是由 $\sigma \mapsto \sigma|_{k_{ab}}$ 定义的 Galois 群自然同态, 而两个行的映射分别是 $\delta_{k'}$ 和 δ_k .

证明 由于 $k \subseteq k' \subseteq \mathcal{Q}_i$, 而 \mathcal{Q}_i 是包含 k' 的 k -有限可分扩域 E 之并集. 从而 $\delta_{k'}$ 和 δ_k 分别是 $\delta_{E/k'}$ 和 $\delta_{E/k}$ 对于 E 的极限. 然后由引理 5 即可证得定理.

注记 这个定理对于任意不必可分的有限扩张 k'/k 也是对的. 但是今后只对于 k'/k 为不分歧扩张的情形用此定理. 参见

§6.2, 定理 3 及其证明.

定理 5 设 k' 是 k 的任意有限可分扩张, 则图表

$$\begin{array}{ccc} U(k) & \xrightarrow{\sim} & \text{Gal}(k_{ab}/k_{nr}) \\ \downarrow & & \downarrow \\ U(k') & \xrightarrow{\sim} & \text{Gal}(k'_{ab}/k'_{nr}) \end{array}$$

是交换的. 其中左边竖线是从 $U(k)$ 到 $U(k')$ 的自然单射, 而右边竖线是上节定义的转移 $i_{k',k}$, 两个行映射为 δ_k 和 $\delta_{k'}$.

证明 与证明定理 4 一样的从引理 7 即得本定理.

系 设 k'/k 为任意有限可分扩张, 则

$$i_{k',k}: \text{Gal}(k_{ab}/k) \rightarrow \text{Gal}(k'_{ab}/k')$$

是单射.

证明 元素 $\sigma \in \text{Gal}(k_{ab}/k)$ 到 $\text{Gal}(Q_s/k)$ 的扩充仍记为 σ , 象上节那样有

$$\sigma_i \sigma = h_i(\sigma) \sigma_i, \quad h(\sigma) = \prod_{i=1}^n h_i(\sigma), \quad n = [k':k],$$

$$i_{k',k}(\sigma) = h(\sigma)|_{k'_{ab}}.$$

又设 $G' = [G, G] = \text{Gal}(Q_s/k_{ab})$ 是 $G = \text{Gal}(Q_s/k)$ 的拓扑换位子群, 于是

$$h(\sigma) = \prod_{i=1}^n \sigma_i \sigma \sigma_i^{-1} \equiv \sigma^n \pmod{G'}.$$

从而

$$i_{k',k}(\sigma)|_{k_{ab}} = \sigma^n.$$

特别若 $i_{k',k}(\sigma) = 1$ 则 $\sigma^n = 1$. 由 §4.2(1) 式给出

$$\tilde{Z} \hookrightarrow \text{Gal}(k_{nr}/k) = \text{Gal}(k_{ab}/k)/\text{Gal}(k_{ab}/k_{nr}),$$

并且不难看出 $\tilde{Z} = \varprojlim \mathbb{Z}/m\mathbb{Z}$ 中只有 1 是有限阶元素. 从而

$\sigma^n = 1$ 导致 $\sigma \in \text{Gal}(k_{ab}/k_{nr})$. 于是

$U(k) \rightarrow U(k')$ 为单射, 从而利用定理 5 即知由 $i_{k',k}(\sigma) = 1$ 推出 $\sigma = 1$.

前面的定理 2 与下章要证明的存在定理 (这是局部类域论的一个基本定理) 本质上是等价的. 证明此定理的一个关键是用引

理 4 将问题归结于 $NU(k_{ab}/k) = 1$ 和 $NU(Q_p/k) = 1$. 在 §5.1 中我们对于任意有限 Galois 扩张 E/k 证明定理 1, 然后在 §5.2 中推导出一系列的引理 (包括引理 4). 正如在 §5.1 末尾所说的, Hazewinkel^[6] 用本节中的方法研究了 Abel 扩张 E/k , 由此立即得到基本等式. 但是还可以用完全不同的方法证明存在定理, 这就是采用第七章中叙述的 Lubin-Tate 形式群方法. 作为 §5.2 和 §5.3 中所述结果的应用, 本书将 Hazewinkel 方法推广到任意 Galois 扩张上, 这一点在 §5.1 中已经谈过 (其证明方法也仅仅复杂一点).

第六章 基本定理

与前面一样令基域为局部域 k , 以 k_{nr} 和 k_{ab} 表示 k 的极大不分歧扩域和极大 Abel 扩域. 前两章论述了扩张 k_{nr}/k 和 k_{ab}/k 的主要性质. 在这个基础上本章首先展示存在由 k 的乘法群 k^\times 到 k_{ab}/k 的 Galois 群 $\text{Gal}(k_{ab}/k)$ 的自然同态

$$\rho_k: k^\times \rightarrow \text{Gal}(k_{ab}/k),$$

然后证明关于 ρ_k 的一系列重要定理. 这些结果形成了局部类域论的核心. 经典意义下的局部类域论基本定理, 即关于 k 的有限 Abe. 扩域的各种定理, 均可由关于 ρ_k 的结果很容易地推导出来.

§ 6.1 基本映射 ρ_k

令

$K = k_{nr}$, $\varphi = K/k$ 的 Frobenius 自同构.

设 ϕ 是 φ 到 $\text{Gal}(k_{ab}/k)$ 的某个扩充, 而令

$$F_\phi = \{\alpha \in k_{ab} \mid \phi(\alpha) = \alpha\},$$

则 F_ϕ 是 k_{ab}/k 的中间域. 从 §4.3, 引理 7 我们有

$$F_\phi \cap K = k, \quad F_\phi K = k_{ab}.$$

从而由 §4.2, 引理 4 可知 $N(F_\phi/k)$ 包含 k 的素元 π .

引理 1 设 ϕ_1, ϕ_2 均是 φ 到 $\text{Gal}(k_{ab}/k)$ 的扩充, 而 π_1, π_2 分别为 $N(F_{\phi_1}/k)$ 和 $N(F_{\phi_2}/k)$ 中所包含的 k 的素元, 令 $\pi_2 = \pi_1 \nu$, $\nu \in U(k)$, 则

$$\phi_1^{-1} \phi_2 = \delta_k(\nu)^{-1}.$$

其中 $\delta_k: U(k) \xrightarrow{\sim} \text{Gal}(k_{ab}/k_{nr})$ 是 §5.3 中定义的拓扑同构.

证明 设 M 是满足 §5.3 中条件 (8) 的域, 而令

$$k_1 = M \cap F_{\phi_1}, \quad k_2 = M \cap F_{\phi_2},$$

$$\varphi_1 = \phi_1|_M, \varphi_2 = \phi_2|_M,$$

则 $\varphi_1|_K = \varphi_2|_K = \varphi$, 从而由 §4.3, 引理 7 可知 k_1 和 k_2 均是 M/k 的补域, 并且

$$k_1 \cap K = k_2 \cap K = k, k_1 K = k_2 K = M,$$

$$\text{Gal}(M/K) \cong \text{Gal}(k_1/k), \text{Gal}(k_2/k),$$

$$[k_1:k] = [k_2:k] = [M:K] < +\infty.$$

此外, φ_1 和 φ_2 分别是 $M = k_{1,ur} = k_{2,ur}$ 对于 k_1 和 k_2 的 Frobenius 自同构. 另一方面, 由于 $\pi_1 \in N(F_{\phi_1}/k)$, $\pi_2 \in N(F_{\phi_2}/k)$, $k \subseteq k_1 \subseteq F_{\phi_1}$, $k \subseteq k_2 \subseteq F_{\phi_2}$, 可知存在 k_1 和 k_2 中的元素 π'_1 和 π'_2 , 使得

$$\pi_1 = N_{k_1/k}(\pi'_1), \pi_2 = N_{k_2/k}(\pi'_2),$$

由于 k_1/k 和 k_2/k 均是完全分歧的, 从而由 §1.3, 定理 3 的系可知 π'_1 和 π'_2 分别是 k_1 和 k_2 的素元. 于是 π'_1 和 π'_2 均是 $M = k_{1,ur} = k_{2,ur}$ 的素元, 从而也是 M 的完备化 \bar{M} 的素元. 因此 $\xi = \pi'_2/\pi'_1 \in U(\bar{M})$, 由于 $\text{Gal}(\bar{M}/K) = \text{Gal}(M/K) \cong \text{Gal}(k_1/k)$ 和 $\text{Gal}(k_2/k)$, 从而

$$N_{\bar{M}/K}(\xi) = N_{k_2/k}(\pi'_2)/N_{k_1/k}(\pi'_1) = \pi_2/\pi_1 = \nu.$$

此外, 由于 $\phi_1|_{k_1} = \phi_2|_{k_2} = 1$, 从而若令 $\sigma = \phi_1^{-1}\phi_2 = \phi_2\phi_1^{-1}$, 则

$$\begin{aligned} \xi^{\varphi_2^{-1}} &= \xi^{\phi_1^{-1}} = (\pi'_2/\pi'_1)^{\phi_1^{-1}} = \pi_1'^{-1}\pi_2 \\ &= \pi_1'/\sigma\phi_1(\pi'_1) = \pi_1'^{1-\sigma}, \sigma \in \text{Gal}(k_{ab}/K). \end{aligned}$$

从而

$$\nu^{-1} = N_{\bar{M}/K}(\xi^{-1}), (\xi^{-1})^{\varphi_2^{-1}} = \pi_1'^{\sigma-1}.$$

将 §5.1, 定理 1 用于 k 的有限 Abe. 扩域 $E = k_2$, $k_0 = E \cap K = k$, $L = EK = k_2K = M$ 以及 $L/E = M/k_2$ 的 Frobenius 自同构 φ_2 和 $L = \bar{M}$ 的素元 π'_1 , 则由同构 $\delta_{E/k} = \delta_{M/k}: U(k)/NU(M/k) \cong \text{Gal}(M/K)$ 给出

$$\nu^{-1} \bmod NU(M/k) \mapsto \sigma|_M.$$

这些对于每个 M 均成立, 从而对于 $\delta_{M/k}$ 的极限 δ_k , 便得到

$$\delta_k(\nu)^{-1} = \delta_k(\nu^{-1}) = \sigma = \phi_1^{-1}\phi_2.$$

引理 2 对于 k 的每个素元 π , 均存在唯一的元素 $\phi \in \text{Gal}(k_{ab}/k)$ 使得

$$\phi|K = \varphi, \pi \in N(F_\varphi/k).$$

如果将这个 ϕ 写成 ϕ_π , 则映射

$$\pi \mapsto \phi_\pi$$

定义出从 k 的素元全体组成的集合 $\{\pi\}$ 到集合 $\{\phi \in \text{Gal}(k_{ab}/k) | \phi \text{ 是 } \varphi \text{ 的扩充}\}$ 之上的满射.

证明 给定 φ 到 $\text{Gal}(k_{ab}/k)$ 的一个扩充 ϕ_0 和包含在 $N(F_{\phi_0}/k)$ 之内的 k 的一个素元 π_0 , 则 k 的每个素元 π 和 φ 到 $\text{Gal}(k_{ab}/k)$ 的每个扩充 ϕ 均可分别唯一地表示成

$$\pi = \pi_0 u, \phi = \phi_0 \sigma, u \in U(k), \sigma \in \text{Gal}(k_{ab}/K).$$

由引理 1 知道, $\pi \in N(F_\varphi/k)$ 的充要条件是 $\delta_k(u)^{-1} = \sigma$. 所以存在唯一的 $\phi = \phi_\pi$ 使得 $\pi \in N(F_\varphi/k)$, 即为

$$\phi_\pi = \phi_0 \delta_k(u)^{-1}.$$

由于 $\delta_k: U(k) \xrightarrow{\sim} \text{Gal}(k_{ab}/K)$ 是同构映射, 即可证明引理的后一半.

引理 3 对于 k 的每个素元 π , 存在唯一的同态

$$\rho: k^\times \rightarrow \text{Gal}(k_{ab}/k)$$

使得

$$\rho(\pi) = \phi_\pi.$$

证明 设 π_0, ϕ_0 如前所述, 则

$$k^\times = \langle \pi_0 \rangle \times U(k), \langle \pi_0 \rangle \xrightarrow{\sim} \mathbb{Z},$$

对于 k^\times 中每个元素 $x = \pi_0^n u$, $n \in \mathbb{Z}$, $u \in U(k)$, 令

$$\rho(x) = \phi_0^n \delta_k(u)^{-1}, \quad (1)$$

这显然定义出同态 $\rho: k^\times \rightarrow \text{Gal}(k_{ab}/k)$. 由引理 2 的证明可知, 对于 k 中素元 $\pi = \pi_0 u$, 我们有

$$\rho(\pi) = \phi_0 \delta_k(u)^{-1} = \phi_\pi.$$

另一方面, 对于 $U(k)$ 中每个元素 u , $\pi = \pi_0 u$ 是 k 的素元并且 $u \mapsto \pi/\pi_0$. 从而 $k^\times = \langle \pi_0 \rangle \times U(k)$ 是由 k 的全部素元之集合 $\{\pi\}$ 所生成的. 所以对于每个素元 π 均满足 $\rho(\pi) = \phi_\pi$ 的同态

ρ 是唯一的.

引理 3 中所述的同态 ρ 由局部域 k 所唯一决定的, 今后记成 ρ_k , 并且叫做是 k 的互反律映射. 范剩余映射或者是 Artin 映射. 本书中我们将它叫作是 k 的基本同态或基本映射.

对于 §5.3 的拓扑同构 δ_k , 我们由 $\delta_k(u) = \delta_k(u)^{-1} (u \in U(k))$ 定义出新的拓扑同构

$$\delta_k: U(k) \xrightarrow{\sim} \text{Gal}(k_{ab}/k_{ur}).$$

然后考查下面的图表:

$$\begin{array}{ccccccc} 1 & \rightarrow & U(k) & \rightarrow & k^\times & \xrightarrow{\nu} & \mathbf{Z} \rightarrow 1 \\ & & \downarrow \delta_k & & \downarrow \rho_k & & \downarrow \varepsilon \\ 1 & \rightarrow & \text{Gal}(k_{ab}/k_{ur}) & \rightarrow & \text{Gal}(k_{ab}/k) & \rightarrow & \text{Gal}(k_{ur}/k) \rightarrow 1 \end{array} \quad (2)$$

其中上面一行是由 k 的正规赋值所定义的正合序列, 下面一行是由 $k \subseteq k_{ur} \subseteq k_{ab}$ 得到的 Galois 群的自然正合序列, 右边映射 ε 是由 §4.2 中所述的同构 $\mathbf{Z} \xrightarrow{\sim} \langle \varphi \rangle$, $n \mapsto \varphi^n$ 所得到的单射. 从 ρ_k 的定义(1)可知

$$\rho_k(u) = \delta_k(u), \quad u \in U(k),$$

因此(2)式左边的四边形是交换的. 另一方面, 设 π 为 k 的素元而 $\rho_k(\pi) = \phi_\pi$, 则

$$\nu(\pi) = 1 \mapsto \varphi = \phi_\pi|_{k_{ur}},$$

从而右边四边形也是交换的, 因此(2)是交换图表.

定理 1 基本映射

$$\rho_k: k^\times \rightarrow \text{Gal}(k_{ab}/k)$$

是从局部紧群 k^\times 到紧群 $\text{Gal}(k_{ab}/k)$ 的连续单射, 它的象是 $\text{Gal}(k_{ab}/k)$ 的稠子群. 并且它诱导出紧子群之间的拓扑同构

$$U(k) \xrightarrow{\sim} \text{Gal}(k_{ab}/k_{ur}).$$

证明 由于(2)中两行均是正合序列, 并且 δ_k, ε 均是单射, 从而 ρ_k 也是单射, 根据 §3.1, 定理 3 知道 $U(k)$ 是 k^\times 的开子群, 而 $\delta_k = \rho_k|_{U(k)}$ 是拓扑同构, 从而 ρ_k 是连续的. 进而, ρ_k 的象包含 $\text{Gal}(k_{ab}/k_{ur})$, 并且 $\varepsilon(\mathbf{Z}) = \langle \varphi \rangle$ 在 $\text{Gal}(k_{ur}/k)$ 中稠密, 从而 ρ_k 的象也是 $\text{Gal}(k_{ab}/k)$ 的稠子群, 定理的后一半是显

然的.

交换图表 (2) 是由基本映射 ρ_k , §4.2 的同构 $Z \rightarrow \langle \varphi \rangle$ 与 §5.3 中同构 δ_k 之变形 δ_k^{-1} 者结合而成的. 但是 ρ_k 并不是由图表 (2) 所唯一决定的. 因为不难看出, 存在其他同态 $k^* \rightarrow \text{Gal}(k_{ab}/k)$, 使得具有与 (2) 类似的交换图表.

§ 6.2 ρ_k 的性质

本节主要是考查局部域 k 的基本映射

$$\rho_k: k^* \rightarrow \text{Gal}(k_{ab}/k)$$

与基域 k 的依赖关系.

假设 (k, ν) , (k', ν') 均是局部域, 而 σ 是从 (k, ν) 到 (k', ν') 的局部域同构, 即同构映射

$$\sigma: k \xrightarrow{\sim} k'$$

满足

$$\nu = \nu' \circ \sigma.$$

又设 Q, Q' 分别是 k, k' 的代数闭包, 而 μ, μ' 分别是 ν, ν' 到 Q, Q' 上的唯一扩充, 同构 $\sigma: Q \xrightarrow{\sim} Q'$ 是 $\sigma: k \xrightarrow{\sim} k'$ 的扩充, 则 $\mu' \circ \sigma$ 显然是 $\nu = \nu' \circ \sigma$ 到 Q' 上的扩充. 从而由 §1.2, 引理 2 可知

$$\mu = \mu' \circ \sigma.$$

不难看出,

$$\sigma: k_{ab} \xrightarrow{\sim} k'_{ab},$$

其中 k_{ab} 是 k 在 Q 中的极大 Abel 扩张, 而 k'_{ab} 是 k' 在 Q' 中的极大 Abel 扩张. 由此得到 Galois 群之间的同构

$$\sigma^*: \text{Gal}(k_{ab}/k) \xrightarrow{\sim} \text{Gal}(k'_{ab}/k')$$

$$\tau \mapsto \sigma \tau \sigma^{-1}.$$

定理 2 图表

$$\begin{array}{ccc} k^* & \rightarrow & \text{Gal}(k_{ab}/k) \\ \downarrow \sigma & & \downarrow \sigma^* \\ k'^* & \rightarrow & \text{Gal}(k'_{ab}/k') \end{array}$$

是交换的. 其中两行映射为 ρ_k 和 $\rho_{k'}$.

证明 根据定义 ρ_k 对于 k 的自然性, 本定理几乎是显然的. 确切地说, σ 将 k_{ab} 映到 k'_{ab} 之上, 设 φ, φ' 分别是 $k_{ab}/k, k'_{ab}/k'$ 的 Frobenius 自同构, 则 $\varphi' = \sigma\varphi\sigma^{-1}$. 又若 π 是 k 的素元, 则 $\pi' = \sigma(\pi)$ 是 k' 的素元, 从上面的注记和 $\phi_{\pi}, \phi_{\pi'}$ 的定义可知 $\phi_{\pi'} = \sigma\phi_{\pi}\sigma^{-1}$. 从而 $\rho_{k'}(\sigma(\pi)) = \sigma\rho_k(\pi)\sigma^{-1}$. 由于 k^{\times} 可由素元集合 $\{\pi\}$ 生成, 从而证明了定理.

现在叙述上面定理的一个特殊情形, 即用于 k 为局部域 k_0 的有限 Galois 扩张的情形. 这时 k_{ab}/k_0 为 Galois 扩张, 并且 $\text{Gal}(k_{ab}/k)$ 是 $\text{Gal}(k_{ab}/k_0)$ 的 Abel 正规子群, 其商群为 $\text{Gal}(k/k_0)$. $\text{Gal}(k_{ab}/k_0)$ 的每个元素 σ 定义出 $\text{Gal}(k_{ab}/k)$ 的自同构

$$\begin{aligned}\sigma^*: \text{Gal}(k_{ab}/k) &\xrightarrow{\sim} \text{Gal}(k_{ab}/k) \\ \tau &\mapsto \sigma\tau\sigma^{-1}\end{aligned}$$

由于 $\text{Gal}(k_{ab}/k)$ 是 Abel 群, 可知 σ^* 只依赖于 $\text{Gal}(k/k_0)$ 中元素 $\sigma|k$. 通过 σ^* 使得 Abel 群 $\text{Gal}(k_{ab}/k)$ 成为 $\text{Gal}(k/k_0)$ 模. 另一方面, $\text{Gal}(k/k_0)$ 以显然方式作用在 k 的乘法群 k^{\times} 上. 将定理 2 用于 $k = k', \mathcal{O} = \mathcal{O}', k_{ab} = k'_{ab}$ 的情形, 可知

$$\rho_k: k^{\times} \rightarrow \text{Gal}(k_{ab}/k)$$

是 $\text{Gal}(k/k_0)$ 模同态.

其次设 k' 是 k 的任意有限扩张, 我们考查 ρ_k 和 $\rho_{k'}$ 的关系. 由于

$$k \subseteq k', k_{ab} \subseteq k'_{ab},$$

从而限制映射 $\sigma \mapsto \sigma|k_{ab}$ 给出自然同态

$$\text{Gal}(k'_{ab}/k') \rightarrow \text{Gal}(k_{ab}/k).$$

最后, 显然有范映射

$$N_{k'/k}: k'^{\times} \rightarrow k^{\times}.$$

定理 3 设 k'/k 是任意有限扩张, 则图表

$$\begin{array}{ccc} k'^{\times} & \rightarrow & \text{Gal}(k'_{ab}/k') \\ \downarrow N_{k'/k} & & \downarrow \\ k^{\times} & \rightarrow & \text{Gal}(k_{ab}/k) \end{array}$$

是交换的,其中两行映射为 $\rho_{k'}$ 和 ρ_k .

证明 设 k'' 是 k'/k 的中间域. 考虑图表

$$\begin{array}{ccc} k'^{\times} & \rightarrow & \text{Gal}(k'_{ab}/k') \\ \downarrow & & \downarrow \\ k''^{\times} & \rightarrow & \text{Gal}(k''_{ab}/k'') \\ \downarrow & & \downarrow \\ k^{\times} & \rightarrow & \text{Gal}(k_{ab}/k) \end{array}$$

左边竖线映射是 $N_{k''/k} \circ N_{k',k''} = N_{k',k}$. 右边映射为限制映射. 如果定理对于扩张 k'/k'' 和 k''/k 均成立,则对于 k'/k 也成立. 特别取 k'' 是 k'/k 的惯性域,由 §3.2, 定理 5 知道 k'/k'' 完全分歧而 k''/k 不分歧. 所以只需要对于 k'/k 完全分歧和不分歧两种情形证明定理即可.

先设 k'/k 是完全分歧的. 令 π' 是 k' 的素元, 则 $\pi = N_{k',k}(\pi')$ 是 k 的素元. 设 φ' 是 k'_{ur}/k' 的 Frobenius 自同构, 令

$$\phi' = \phi_{\pi'} = \rho_{k'}(\pi'), \quad F' = F_{\phi'}.$$

由引理 2 和 $\phi_{\pi'}$ 的定义可知

$$\phi'|_{k'_{ur}} = \varphi', \quad \pi' \in N(F'/k').$$

由于 k'/k 完全分歧, 如果设 φ 是 k_{ur}/k 的 Frobenius 自同构, 则 $\varphi'|_{k_{ur}} = \varphi$, 从而若令

$$F = F' \cap k_{ab}, \quad \phi = \phi'|_{k_{ab}},$$

则

$$\begin{aligned} F &= F_{\phi}, \quad \phi|_{k_{ur}} = \phi'|_{k_{ur}} \quad (\phi'|_{k'_{ur}})|_{k_{ur}} \\ &= \varphi'|_{k_{ur}} = \varphi. \end{aligned}$$

另一方面, 由 $\pi' \in N(F'/k')$ 显然得出 $\pi = N_{k',k}(\pi') \in N(F'/k)$, 从而

$$\pi \in N(F/k).$$

因此由 ϕ_{π} 的定义可知 $\phi = \phi_{\pi} = \rho_k(\pi)$, 即

$$\rho_k(N_{k',k}(\pi')) = \phi = \rho_{k'}(\pi')|_{k_{ab}}.$$

由于 k'^{\times} 由素元集合 $\{\pi'\}$ 生成, 从而在 k'/k 完全分歧的情形定理得到证明.

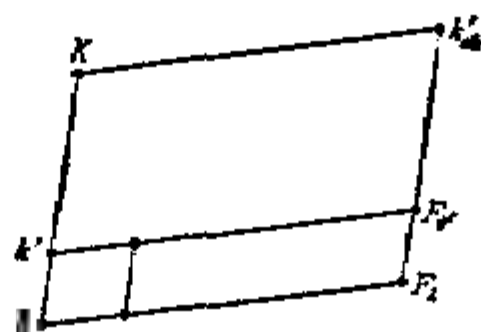
其次设 k'/k 为不分歧扩张, 令 $\pi = [k':k]$. 取 π 为 k 的素元, $\phi = \phi_\pi = \rho_k(\pi)$. 这时, 由于 k'/k 是 Galois 扩张, 则 k'_{ab}/k 也是 Galois 扩张, 设 λ 为 ϕ 到 $\text{Gal}(k'_{ab}/k)$ 的扩充: $\lambda|_{k_{ab}} = \phi$. 取

$$F_1 = \{\alpha' \in k'_{ab}, \lambda(\alpha') = \alpha'\},$$

则 $\lambda|_K = \phi|_K = \varphi$, 从而由 §4.3, 引理 7 得到

$$F_1 \cap K = k, \quad F_1 K = k'_{ab},$$

$$\text{Gal}(k'_{ab}/F_1) \cong \text{Gal}(K/k).$$



令 $\phi' = \lambda^\pi$, $\varphi' = \varphi^\pi$, 则 $\phi'|_K = \varphi'$, 从而由

$$k \subseteq k' \subseteq K, [k':k] = \pi, K = k'_{ab}$$

可知 φ' 是 K/k' 的 Frobenius 自同构, 而 ϕ' 是它到 $\text{Gal}(k'_{ab}/k')$ 的扩充. 另一方面, 由于 $\text{Gal}(k'_{ab}/F_1) \cong \text{Gal}(K/k)$, 从而得到

$$k' F_1 = F_{\psi'} = \{\alpha' \in k'_{ab} | \phi'(\alpha') = \alpha'\}.$$

由 $F_1 \cap K = k$ 和 §4.2, 引理 4 可知 $N(F_1/k)$ 包含 k 的素元 π_1 , 由 $F_\psi = k'_{ab} \cap F_1 \subseteq F_1$ 可知 $\pi_1 \in N(F_\psi/k)$. 又由 $\phi = \phi_\pi$ 可知 $\pi \in N(F_\psi/k)$, 再由引理 2 即知 $\pi_1 = \pi$, 从而 $\pi \in N(F_1/k)$. 此外, 由于 $F_1 \cap K = k$, 可知 $\{\tilde{k} | k \subseteq \tilde{k} \subseteq F_1, [\tilde{k}:k] < +\infty\}$ 和 $\{\tilde{k}' | k' \subseteq \tilde{k}' \subseteq k' F_1, [\tilde{k}':k'] < +\infty\}$ 是一一对应的. 从而由 $\pi \in N(F_1/k)$ 可得 $\pi \in N(k' F_1/k')$. 特别地, k 的素元 π 也是不分歧扩张 k' 的素元, 因此

$$\varphi|_K = \varphi', \quad \pi \in N(k' F_1/k') = N(F_{\psi'}/k').$$

所以由定义可知

$$\rho_{k'}(\pi) = \phi' = \lambda^\pi,$$

从而得到

$$\begin{aligned}\rho_k(\pi)|_{k_{ab}} &= \lambda^n|_{k_{ab}} \quad \psi^n = \rho_k(\pi)^n \\ &= \rho_k(N_{k'/k}(\pi)).\end{aligned}$$

对于 $u' \in U(k')$, $u \in U(k)$ 令

$$\rho_{k'}(u') = \delta_{k'}(u')^{-1}, \quad \rho_k(u) = \delta_k(u)^{-1}.$$

又因为 k'/k 是 Galois 扩张, 从而由 §5.3, 定理 4 知道

$$\rho_{k'}(u')|_{k_{ab}} = \rho_k(N_{k'/k}(u')).$$

再由 $k'^\times = \langle \pi \rangle \times U(k')$ 即知定理对于不分歧扩张 k'/k 也是对的。

现在考虑 k'/k 是有限可分扩张的情形。这时由 §5.2 知道可定义从 k 到 k' 的 Galois 群的转移:

$$t_{k'/k}: \text{Gal}(k_{ab}/k) \rightarrow \text{Gal}(k_{ab}/k').$$

又显然地定义自然单射

$$k^\times \rightarrow k'^\times.$$

我们分几步来证明图表

$$\begin{array}{ccc} k^\times & \rightarrow & \text{Gal}(k_{ab}/k) \\ \downarrow & & \downarrow t_{k'/k} \\ k'^\times & \rightarrow & \text{Gal}(k'_{ab}/k') \end{array}$$

是交换的。为简单起见, 今后将此图表记为 (k'/k) 。

引理 4 设 k' 是有限可分扩张 k''/k 的中间域: $k \subseteq k' \subseteq k''$ 。

i) 如果图表 (k''/k') 和 (k'/k) 均是交换的, 则 (k''/k) 也是交换的。

ii) 如果图表 (k'/k) 和 (k''/k') 均是交换的, 则 (k''/k) 也是交换的。

证明 考虑将 (k'/k) 与 (k''/k') 合成后的图表:

$$\begin{array}{ccc} k^\times & \rightarrow & \text{Gal}(k_{ab}/k) \\ \downarrow & & \downarrow \\ k'^\times & \rightarrow & \text{Gal}(k'_{ab}/k') \\ \downarrow & & \downarrow \\ k''^\times & \rightarrow & \text{Gal}(k''_{ab}/k'') \end{array}$$

由于 $t_{k''/k} = t_{k''/k'} \circ t_{k'/k}$, 上面图表的最外圈的大四边形即是图表 (k''/k) 。由此即证 i)。再由 §5.3, 定理 5 的系可知 $t_{k''/k'}$ 为单

射,由此和上面图表即得到 ii).

引理 5 如果 k'/k 为有限 Galois 扩张,则对于每个元素 $x \in N(k'/k)$, 图表 (k'/k) 是交换的, 即 x 在 $\text{Gal}(k_{ab}/k)$ 上的两个路径的象是一致的.

证明 假设 $x = N_{k'/k}(x')$, $x' \in k'^{\times}$, 即

$$x = \prod_{\tau} \tau(x'), \tau \in \text{Gal}(k'/k).$$

令 $\sigma = \rho_{k'}(x')$, 并且 τ 到 $\text{Gal}(k_{ab}/k)$ 的扩充仍记为 τ , 将定理 2 后面的注记用于 $k \subseteq k' \subseteq k_{ab}$, 得到

$$\rho_k(x) = \prod_{\tau} \tau \sigma \tau^{-1}.$$

另一方面, 这时 $H = \text{Gal}(Q/k')$ 是 $G = \text{Gal}(Q/k)$ 的正规子群, 将 τ 到 $\text{Gal}(Q/k)$ 的扩充仍记为 τ , 则 $\text{Gal}(k'/k)$ 的全部元素到 $G = \text{Gal}(Q/k)$ 的扩充所构成的集合 $\{\tau\}$ 是 G 关于 H 的陪集代表元系, 再由 §5.2 中所述的转移映射 $i_{k'/k} = i_{G,H}$ 的定义, 可知

$$i_{k'/k}(\sigma|k_{ab}) = \prod_{\tau} \tau \sigma \tau^{-1}.$$

再由定理 3 知道 $\sigma|k_{ab} = \rho_{k'}(x')$, $k_{ab} = \rho_k(N_{k'/k}(x')) = \rho_k(x)$, 因此

$$\rho_{k'}(x) = i_{k'/k}(\rho_k(x)),$$

这就证明了引理的论断.

定理 4 设 k' 为 k 的任意有限可分扩张, 则图表

$$\begin{array}{ccc} k^{\times} & \rightarrow & \text{Gal}(k_{ab}/k) \\ \downarrow & & \downarrow i_{k/k} \\ k'^{\times} & \rightarrow & \text{Gal}(k'_{ab}/k') \end{array}$$

是交换的, 其中行映射为 ρ_k 和 $\rho_{k'}$.

证明 设 E 是 k 的 Galois 扩张并且包含 k' : $k \subseteq k' \subseteq E$. 由引理 4 ii) 知道, 如果定理对于 E/k 和 E/k' 成立, 则对于 k'/k 也成立. 从而以下只考虑 k/k 为 Galois 扩张的情形即可. 设 k_0 是 k/k 的惯性域, 则由 §3.2, 定理 5 可知 k'/k_0 完全分歧而 k/k 不

分歧, 因此又不妨假定 k'/k 是完全分歧或者不分歧的 Galois 扩张.

先设 k'/k 完全分歧. 令 π' 为 k' 的素元, 则 $\pi = N_{k'/k}(\pi')$ 是 k 的素元, 并且

$$k^\times = \langle \pi \rangle \times U(k).$$

由引理 5 知道定理 4 中的图表对于 π 是交换的, 又由于 $\rho_k|U(k) = \delta_k$, 从而由 §5.3, 定理 5 可知此图表对于 $U(k)$ 中元素也是交换的. 于是在这种情形下定理成立.

其次设 k'/k 不分歧. 由于 k^\times 由它的素元集合生成, 从而只需对于 k 的每个素元 π 证明图表交换即可. 采用与定理 3 的证明后半相同的记号, 并且设 λ 是 $\phi = \rho_k(\pi)$ 到 $\text{Gal}(k_{ab}/k)$ 的扩充, 于是

$$\rho_{k'}(\pi) = \lambda^\pi, \quad \pi = [k':k].$$

设 φ 是 $K, k(-k_{ab}/k)$ 的 Frobenius 自同构, 则由 ϕ 的定义知

$$\lambda|K = \phi|K = \varphi,$$

从而 $\{1, \lambda, \dots, \lambda^{\pi-1}\}$ 形成 $\text{Gal}(k_{ab}/k)$ 对于 $\text{Gal}(k'_{ab}/k')$ 的陪集代表元系. 由转移的定义易知

$$t_{k'/k}(\phi) = \lambda^\pi.$$

从而

$$\rho_{k'}(\pi) = t_{k'/k}(\rho_k(\pi)).$$

这就证明了定理.

将转移 $t_{k'/k}$ 的定义稍加变化, 即可把上面定理推广到任意 (不必可分的) 有限扩张 k'/k 上. 其方法如下所示: 设 k'' 是 k 在 k' 中的极大可分扩域, 即 $k' = k' \cap \bar{Q}$, 令 $m = [k':k'']$. 如果 k 的特征为 0, 则 $m = 1$. 而如果 k 的特征为 p , 则 m 必为 p 的幂. 无论是哪种情形, 映射 $\alpha \mapsto \alpha^{1/m}$ 定义出代数封闭域 \bar{Q} 的自同构:

$$\omega_m: \bar{Q} \xrightarrow{\sim} \bar{Q}.$$

根据 §3.3, 引理 5 可知 k'/k'' 为完全分歧扩张. 因此

$$\omega_m|k' \xrightarrow{\sim} k',$$

所以若令 ν' 和 ν'' 分别是 k' 和 k'' 的正规赋值, 则

$$\nu'' = \nu' \circ \omega_m.$$

因此, 若对于元素 $\tau \in \text{Gal}(k''/k')$ 令 $\omega_m^*(\tau) = \omega_m \tau \omega_m^{-1}$, 则由定理 2 可知图表

$$\begin{array}{ccc} k''^{\times} & \rightarrow & \text{Gal}(k''/k') \\ \downarrow \omega_m & & \downarrow \omega_m^* \\ k^{\times} & \rightarrow & \text{Gal}(k/k) \end{array}$$

是交换的. 因此当 $x \in k'$ 时,

$$\rho_{k'}(x^{1/m}) = \omega_m(\rho_{k''}(x))\omega_m^{-1},$$

从而

$$\rho_{k'}(x) = \omega_m(\rho_{k''}(x)^m)\omega_m^{-1}.$$

如果又若 $x \in k^{\times}$, 则由定理 4 知道 $\rho_{k''}(x) = \iota_{k''/k}(\rho_k(x))$, 再由上式即得到

$$\rho_{k'}(x) = \omega_m(\iota_{k''/k}(\rho_k(x)^m))\omega_m^{-1}.$$

因此对于扩张 k'/k 若由

$$\iota_{k'/k}(\sigma) = \omega_m(\iota_{k''/k}(\sigma^m))\omega_m^{-1}, \quad \sigma \in \text{Gal}(k/k)$$

定义出转移

$$\iota_{k'/k}: \text{Gal}(k/k) \rightarrow \text{Gal}(k'/k),$$

则定理 4 的图表

$$\begin{array}{ccc} k^{\times} & \rightarrow & \text{Gal}(k/k) \\ \downarrow & & \downarrow \\ k'^{\times} & \rightarrow & \text{Gal}(k'/k) \end{array}$$

在这种情形下是交换的. 不难看出, 上述的 $\iota_{k',k}$ 是可分扩张情形下定义的转移的推广. 此外, $\iota_{k/k}$ 是单射 (注意若 k 的特征为 p , 则 $U(k)$ 包含 p 次本原单位根), 并且容易证明, 对于任意有限扩张 $k \subseteq k' \subseteq k''$ 有 $\iota_{k''/k} = \iota_{k''/k'} \circ \iota_{k'/k}$.

定理 5 为了同态

$$\kappa: k^{\times} \rightarrow \text{Gal}(k/k)$$

与 k 的基本映射 ρ_k 一致, 其充分必要条件是 κ 具有如下两条性质:

- i) 对于 k 的每个素元 π 均有 $\kappa(\pi) \neq 1$;

ii) 对于 k 的任意有限 Abel 扩张 k' , 均有 $\kappa(N(k'/k)) \subset \text{Gal}(k_{ab}/k')$, 即对于每个 $x \in N(k'/k)$ 均有 $\kappa(x)|_{k'} = 1$.

证明 由引理 3 以及 $\rho = \rho_k$ 的定义即知 ρ_k 满足 i). 此外, 由于 k'/k 是 Abel 扩张, 所以 $k \subset k' \subset k_{ab}$, 从而由定理 3 的图表可知 $\text{Gal}(k'_{ab}/k') \rightarrow \text{Gal}(k_{ab}/k)$ 的象包含在 $\text{Gal}(k_{ab}/k')$ 之中. 再由定理 3 即知 ρ_k 也满足 ii). 反之, 假设 κ 是满足条件 i) 和 ii) 的任意同态. 对于 k 中任意素元 π 令 $\phi = \phi_\pi = \rho_k(\pi)$, 由 ϕ_π 和 F_ϕ 的定义可知 $\pi \in N(F_\phi/k)$, $\phi|_{F_\phi} = 1$. 所以如果设 k' 是 k 的任意有限扩域并且包含在 F_ϕ 之中, 则 $\pi \in N(k'/k)$, 所以由假设条件 ii) 得出 $\kappa(\pi)|_{k'} = 1$. 由于 F_ϕ 是所有这样的 k' 的并集合, 从而

$$\kappa(\pi)|_{F_\phi} = 1 = \rho_k(\pi)|_{F_\phi}.$$

另一方面, 由假设条件 i) 可知 $\kappa(\pi)|_K = \rho_k(\pi)|_K$, $K = \varphi(K = k_{ur})$, 而由 §4.3, 引理 7 有 $k_{ab} = F_\phi K$, 从而得到

$$\kappa(\pi) = \rho_k(\pi).$$

由于 k^\times 是由素元集合 $\{\pi\}$ 生成的, 从而 $\kappa = \rho_k$, 即证明了定理.

§ 6.3 有限 Abel 扩域

本节中证明关于局部域 k 的有限扩域, 特别是有限 Abel 扩域的基本结果.

定理 6 设 k' 是局部域 k 的任意有限扩域, 则基本映射 $\rho_k: k^\times \rightarrow \text{Gal}(k_{ab}/k)$ 诱导出商群同构

$$\rho_{k'/k}: k^\times / N(k'/k) \xrightarrow{\sim} \text{Gal}(k_{ab} \cap k'/k),$$

并且

$$N(k'/k) = \rho_k^{-1}(\text{Gal}(k_{ab}/k_{ab} \cap k')),$$

$$\text{Gal}(k_{ab}/k_{ab} \cap k') = \rho_k(N(k'/k))$$

在 $\text{Gal}(k_{ab}/k)$ 中的闭包.

证明 对于局部域 k' 可以定义与 (2) 一样的交换图表

$$\begin{array}{ccccccc} 1 & \rightarrow & U(k') & \rightarrow & k^{\times} & \rightarrow & \mathbf{Z} \rightarrow 1 \\ & & \downarrow \delta_k & & \downarrow \rho_k & & \downarrow \sigma' \end{array} \quad (3)$$

$$1 \rightarrow \text{Gal}(k'_{ab}/k'_{ur}) \rightarrow \text{Gal}(k'_{ab}/k') \rightarrow \text{Gal}(k'_{ur}/k') \rightarrow 1$$

又从(3)上行正合序列和(2)上行正合序列得到交换图表

$$\begin{array}{ccccccc} 1 & \rightarrow & U(k') & \rightarrow & k'^{\times} & \rightarrow & \mathbf{Z} \rightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow f \\ 1 & \rightarrow & U(k) & \rightarrow & k^{\times} & \rightarrow & \mathbf{Z} \rightarrow 1 \end{array} \quad (4)$$

其中中间竖线映射是范映射 $N_{k'/k}$, 而 $f \mapsto f(k'/k)$ 表示映射 $a \mapsto fa$. 同样地, 从(3)的下行正合序列和(2)的下行正合序列由 Galois 群之间的自然同态定义出交换图表

$$\begin{array}{ccccccc} 1 & \rightarrow & \text{Gal}(k'_{ab}/k'_{ur}) & \rightarrow & \text{Gal}(k'_{ab}/k') & \rightarrow & \text{Gal}(k'_{ur}/k') \rightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \rightarrow & \text{Gal}(k_{ab}/k_{ur}) & \rightarrow & \text{Gal}(k_{ab}/k) & \rightarrow & \text{Gal}(k_{ur}/k) \rightarrow 1 \end{array} \quad (5)$$

令 φ, φ' 分别为 $k_{ur}/k, k'_{ur}/k'$ 的 Frobenius 自同构, 由于 $[k_{ur} \cap k': k] = f$, 从而 $\varphi|_{k_{ur}} = \varphi'$. 利用 §5.3, 定理 4 和 §6.2, 定理 3 即可把 (2), (3), (4), (5) 合成为立体的交换图表. 于是由(4)的余核和(5)的余核定义出的图表

$$\begin{array}{ccccccc} 1 & \rightarrow & U(k), NU(k'/k) & \rightarrow & k^{\times}/N(k'/k) & \rightarrow & \mathbf{Z}/f\mathbf{Z} \rightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \rightarrow & \text{Gal}(k_{ab} \cap k'_{ur}/k_{ur}) & \rightarrow & \text{Gal}(k_{ab} \cap k'/k) & \rightarrow & \text{Gal}(k_{ur} \cap k'/k) \rightarrow 1 \end{array} \quad (6)$$

也是交换的. 而且两行均是正合序列. 左边竖线是由同构映射 $\delta_k, \delta_{k'}$ 得到的同构, 右边竖线是由 $\varphi|(k_{ur} \cap k')$ 生成的 f 阶循环群 $\text{Gal}(k_{ur} \cap k'/k)$ 上的同构. 因此中间竖线也是同构:

$$k^{\times}/N(k'/k) \xrightarrow{\sim} \text{Gal}(k_{ab} \cap k'/k).$$

这个同构是由基本映射 $\rho_k: k^{\times} \rightarrow \text{Gal}(k_{ab}/k)$ 诱导出来的, 但是

$$\text{Gal}(k_{ab} \cap k'/k) = \text{Gal}(k_{ab}/k), \text{Gal}(k_{ab}/k_{ab} \cap k'),$$

从而

$$N(k'/k) = \rho_k^{-1}(\text{Gal}(k_{ab}/k_{ab} \cap k')).$$

此外, ρ_k 将 $k^{\times}/N(k'/k)$ 的每个陪集映到 $\text{Gal}(k_{ab}/k)/\text{Gal}(k_{ab}/k_{ab} \cap k')$ 所对应的陪集中. 但是从定理 1 知道 $\rho_k(k^{\times})$ 在 $\text{Gal}(k_{ab}/$

k) 中稠密, 从而 $\text{Gal}(k_{ab}/k)/\text{Gal}(k_{ab}/k_{ab} \cap k')$ 的有限个闭集均是 $\text{Gal}(k_{ab}/k)$ 的闭集合, 因此 $\text{Gal}(k_{ab}/k_{ab} \cap k')$ 是 $\rho_k(N(k'/k))$ 的闭包.

由于 ρ_k 是连续同态, 从上述定理可知 $N(k'/k)$ 是 k^\times 的闭子群并且指数有限, 从而也是开子群. 这就又证明了 §3.3, 定理 7. 特别当 k'/k 是 Abel 扩张时, 立刻得到如下定理:

定理 7 设 k' 是局部域 k 的任意有限 Abel 扩域, 则基本映射 $\rho_k: k^\times \rightarrow \text{Gal}(k_{ab}/k)$ 诱导出商群同构

$$\rho_{k'/k}: k^\times/N(k'/k) \rightarrow \text{Gal}(k'/k).$$

从而有

$$[k^\times: N(k'/k)] = [k': k].$$

这一定理是关于局部域的有限 Abel 扩域的最基本结果. 而定理中的等式叫作是局部类域论的基本等式. 这一点在 §5.1 末尾曾经谈过. 那里还提到过, 对于 Abel 扩张从 §5.1 的交换图表并使用 §5.1, 引理 1 和蛇形引理容易得到基本等式一个直接证明. 定理 7 即是所谓的同构定理, 即有限 Abel 群 $k^\times/N(k'/k)$ 和 $\text{Gal}(k'/k)$ 是同构的. 这是一个相当深刻的结果.

定理 8 (终结定理) 设 k' 是局部域 k 的任意有限扩域, k'' 是 k 的有限 Abel 扩域, 则

$$N(k'/k) \subseteq N(k''/k) \iff k'' \subseteq k'.$$

特别地有

$$N(k'/k) = N(k''/k) \iff k'' = k' \cap k_{ab}.$$

证明 由于 k''/k 是 Abel 扩张, 从而 $k'' \subseteq k'$ 等价于 $k'' \subseteq k_{ab} \cap k'$. 因此又与 $\text{Gal}(k_{ab}/k_{ab} \cap k') \subseteq \text{Gal}(k_{ab}/k'')$ 等价. 将定理 6 后一半中的等式用于 k'/k 和 k''/k 即得到定理.

系 设 k'/k 为任意有限扩张, 则

$$N(k'/k) = N(k_{ab} \cap k'/k), [k^\times: N(k'/k)] \leq [k': k].$$

并且后者等式成立的充要条件是 k'/k 为 Abel 扩张.

证明 第一个等式已如定理 8 中所述. 将基本等式用于 Abel 扩张 $k_{ab} \cap k'/k$, 则有

$$[k^x:N(k/k)] = [k^x:N(k_{ab} \cap k'/k)] \\ = [k_{ab} \cap k':k] \leq [k':k].$$

并且等号成立 $\Leftrightarrow k_{ab} \cap k' = k' \Leftrightarrow k'/k$ 为 Abel 扩张.

如果 k''/k 为任意有限扩张, k' 是 k''/k 的中间域, 即 $k \subseteq k' \subseteq k''$, 考查图表

$$\begin{array}{ccc} k^x/N(k''/k) & \xrightarrow{\sim} & \text{Gal}(k_{ab} \cap k''/k) \\ \downarrow & & \downarrow \\ k^x/N(k'/k) & \xrightarrow{\sim} & \text{Gal}(k_{ab} \cap k'/k) \end{array}$$

其中两行映射分别为 $\rho_{k''/k}$ 和 $\rho_{k'/k}$, 而两竖线映射分别是由 $N(k''/k) \subseteq N(k'/k) \subseteq k^x$ 和 $k \subseteq k_{ab} \cap k' \subseteq k_{ab} \cap k''$ 给出的自然同态.

引理 6 上面的图表是交换的, 从而

$$\rho_{k''/k}(N(k'/k)/N(k''/k)) = \text{Gal}(k_{ab} \cap k''/k_{ab} \cap k').$$

证明 由于 $\rho_{k''/k}$ 和 $\rho_{k'/k}$ 均是基本映射 $\rho_k: k^x \rightarrow \text{Gal}(k_{ab}/k)$ 诱导出来的同构, 即可知道上面图表是交换的. 于是诱导出竖线映射的余核之间的同构

$$N(k/k)/N(k''/k) \xrightarrow{\sim} \text{Gal}(k_{ab} \cap k''/k_{ab} \cap k').$$

从而引理的后一部分也成立.

定理 9 设 k' 是局部域 k 的任意有限扩域, k_0 是 k'/k 的惯性域, 即 $k_0 = k_{ur} \cap k'$, 则

$$N(k_0/k) = U(k)N(k'/k),$$

$$\rho_{k_0/k}: k^x/U(k)N(k'/k) \xrightarrow{\sim} \text{Gal}(k_0/k).$$

并且对于 k 的任意素元 π , $\rho_{k_0/k}$ 将 $\pi U(k)N(k'/k)$ 映成不分歧扩张 k_0/k 的 Frobenius 自同构, 所以 k'/k 的剩余类次数 $f(k'/k)$ 等于 $\pi U(k)N(k'/k)$ 在 $k^x/U(k)N(k'/k)$ 中的阶数.

证明 从交换图表 (6) 可知中间竖线映射 $\rho_{k'/k}$ 将 $U(k)/NU(k'/k) \rightarrow k^x/N(k'/k)$ 的象映成 $\text{Gal}(k_{ab} \cap k/k) \rightarrow \text{Gal}(k_{ur} \cap k'/k)$ 的核, 即

$$\rho_{k'/k}(U(k)N(k'/k)/N(k'/k)) = \text{Gal}(k_{ab} \cap k'/k_0).$$

注意 $k_0 = k_{ab} \cap k_0$, 而 $\rho_{k'/k}$ 是同构, 从而由上一引理即得到

$$N(k_0/k) = U(k)N(k'/k).$$

由定理 5 知道 $\rho_k(\pi)|_{k_{\infty}}$ 是 k_{∞}/k 的 Frobenius 自同构, 而 $\rho_{k_0/k}$ 是 ρ_k 诱导出来的同构, 即知定理后一半也是对的. 最后再注意 $\text{Gal}(k_0/k)$ 是由 Frobenius 自同构生成的 $f(k'/k)$ 阶循环群.

系 设 k' 是局部域 k 的有限扩张, 则

$$k'/k \text{ 为不分歧扩张} \iff U(k) \subseteq N(k'/k),$$

$$k'/k \text{ 为完全分歧扩张} \iff k^{\times} = U(k)N(k'/k).$$

证明 由于 k_0/k 是 Abel 扩张, 并且 $N(k_0/k) = U(k)N(k'/k)$, 从而由定理 8 得到

$$\begin{aligned} k_0 = k' &\iff U(k)N(k'/k) = N(k'/k) \\ &\iff U(k) \subseteq N(k'/k), \end{aligned}$$

$$k_0 = k \iff U(k)N(k'/k) = N(k/k) = k^{\times}.$$

引理 7 设 H 为局部紧群 k^{\times} 的闭子群并且 $[k^{\times}:H] < +\infty$, 则存在 k 的有限 Abel 扩张 k' 使得

$$\Lambda(k'/k) \subseteq H \subseteq k^{\times}.$$

证明 由 §5.3, 定理 2 可知

$$NU(k_{ab}/k) = \bigcap_E NU(E/k) = 1,$$

其中 E 过 k 的全部有限 Abel 扩张. 由于 H 为 k^{\times} 的开子群, 因此 $H \cap U(k)$ 也是 $U(k)$ 的开子群. 再注意到 $U(k)$ 是紧群而 $NU(E/k)$ 为 $U(k)$ 的闭子群, 即知存在 E 满足

$$NU(E/k) \subseteq H \cap U(k) \subseteq H.$$

令 $n = [k^{\times}:H]$ 并设 k' 是 E 的 n 次不分歧扩张, 则 $E_{\infty} = Ek_{\infty}$ 是 k 的 Abel 扩张, 从而 k'/k 为有限 Abel 扩张. 由于 k'/E 是不分歧扩张, 由 §3.3, 引理 4 可知 $NU(k'/E) = U(E)$. 从而

$$N_{k'/k}(U(k')) = N_{k'/k}(U(E)) = NU(E/k) \subseteq H.$$

另一方面, E 的素元 π' 同时也是 k' 的素元, 从而

$$N_{k'/k}(\pi') = N_{E/k}(\pi')^n \in H.$$

再由 $k^{\times} = \langle \pi' \rangle \times U(k')$ 即知 $N(k'/k) \subseteq H$.

定理 10 (存在定理) 设 H 是局部域 k 的乘法群 k^{\times} 的闭子群并且 $[k^{\times}:H] < +\infty$, 则存在 k 的唯一的有限 Abel 扩张 k' 使

得

$$N(k'/k) = H.$$

证明 由引理 7 知道存在有限 Abel 扩张 k''/k 使得

$$N(k''/k) \subseteq H \subseteq k^\times.$$

由于 $\rho_{k'',k}: k^\times/N(k''/k) \xrightarrow{\sim} \text{Gal}(k''/k)$ 将 $H/N(k''/k)$ 映成 $\text{Gal}(k''/k)$ 的子群, 由 Galois 理论可知存在 k''/k 的中间域 k' , 使得

$$\rho_{k'',k}(H/N(k''/k)) = \text{Gal}(k''/k').$$

将引理 6 用于 Abel 扩张 k''/k 的中间域 k' , 则

$$\rho_{k'',k}(N(k'/k), N(k''/k)) = \text{Gal}(k''/k').$$

由于 $\rho_{k''/k}$ 是同构映射, 因此得到

$$N(k'/k) = H.$$

由定理 8 可知 k' 的唯一性.

从上面的证明可以看出, 由 §5.3, 定理 2 推导出引理 7 以及由引理 7 推导出存在定理都很容易. 另一方面, 从引理 7 或者定理 10 显然也可以证得 §5.3, 定理 2. 所以正如 §5.3 末尾所说过的, §5.3 定理 2 和上面的存在定理本质上是等价的.

从定理 10 可知, 对应

$$k' \mapsto H = N(k'/k)$$

定义出从集合 $\{k' | k'/k \text{ 为有限 Abel 扩张}\}$ 到集合 $\{H | H \text{ 为 } k^\times \text{ 的闭子群, } [k^\times:H] < +\infty\}$ 之上的满射. 并且由定理 8 知道这个对应与包含关系是反序的. 从而如果 $k_1 \mapsto H_1$, $k_2 \mapsto H_2$, 则

$$k_1 \cap k_2 \mapsto H_1 H_2, \quad k_1 k_2 \mapsto H_1 \cap H_2.$$

又由引理 6 可知, 如果 $k_1 \subset k_2$, $H_2 \subset H_1$, 则有交换图表:

$$\begin{array}{ccc} k^\times/H_2 & \xrightarrow{\sim} & \text{Gal}(k_2/k_1) \\ \downarrow & & \downarrow \\ k^\times/H_1 & \xrightarrow{\sim} & \text{Gal}(k_1/k) \end{array} \quad (7)$$

其中诸映射如引理 6 所述. 由于 k_{ab} 是全部有限 Abel 扩域 k' 之并, 由 §4.1 的注记可知 $\text{Gal}(k_{ab}/k)$ 是 (7) 式右边同态族 $\text{Gal}(k'/k)$ 的射影极限:

$$\text{Gal}(k_{ab}/k) = \varinjlim \text{Gal}(k'/k).$$

而对于(7)式左边的同态,若令

$$\tilde{k}^x = \varinjlim k^x/H,$$

则由 $\rho_k: k \rightarrow \text{Gal}(k_{ab}/k)$ 得到射影有限群的拓扑同构

$$\bar{\rho}_k: \tilde{k}^x \xrightarrow{\sim} \text{Gal}(k_{ab}/k).$$

由自然同态 $k^x \rightarrow k^x/H$ 定义出单射

$$k^x \rightarrow \tilde{k}^x,$$

而每个 $\rho_{k'/k}$ 是由基本映射 $\rho_k: k^x \rightarrow \text{Gal}(k_{ab}/k)$ 诱导出来的同构,从而合成映射

$$k^x \rightarrow \tilde{k}^x \xrightarrow{\sim} \text{Gal}(k_{ab}/k)$$

与 ρ_k 一致. 另一方面,对图表(5)各项作射影极限,即得到交换图表

$$\begin{array}{ccccccc} 1 \rightarrow & U(k) & \rightarrow & \tilde{k}^x & \rightarrow & \tilde{Z} & \rightarrow 1 \\ & \downarrow & & \downarrow & & \downarrow & \\ 1 \rightarrow & \text{Gal}(k_{ab}/k_{ur}) & \rightarrow & \text{Gal}(k_{ab}/k) & \rightarrow & \text{Gal}(k_{ur}/k) & \rightarrow 1 \end{array} \quad (8)$$

其中左边竖线是拓扑同构 $\bar{\rho}_k$, 右边则是 §4.2 的拓扑同构(1). 又由于此图表下行显然是正合序列,从而上行也是正合序列.(一般情形下,射影极限并不保存序列的正合性.但是我们这里是有限群(紧群)的极限,即可知上行也是正合的.)由(8)定义出交换图表

$$\begin{array}{ccccccc} 1 \rightarrow & U(k) & \rightarrow & k^x & \rightarrow & Z & \rightarrow 1 \\ & & & \downarrow & & \downarrow & \\ 1 \rightarrow & U(k) & \rightarrow & \tilde{k}^x & \rightarrow & \tilde{Z} & \rightarrow 1 \\ & \downarrow & & \downarrow & & \downarrow & \\ 1 \rightarrow & \text{Gal}(k_{ab}/k_{ur}) & \rightarrow & \text{Gal}(k_{ab}/k) & \rightarrow & \text{Gal}(k_{ur}/k) & \rightarrow 1 \end{array}$$

此图表的各行均是正合序列.根据上面所述,将上行和下行放在一起的图表恰好是 §6.1 的图表(2). 与(2)中一样,交换图表(8)是将 §4.2 的拓扑同构(1)和 §5.3 的拓扑同构 $\bar{\rho}_k$ 的变形 $\bar{\rho}_k$ 结合而成的. 又由 §4.3, 引理 7 之前所叙述的注记可知,从(8)的上行正合序列给出紧群同构

$$\tilde{k}^x \xrightarrow{\sim} \tilde{Z} \times U(k).$$

从而得到

$$\mathrm{Gal}(k_{ab}/k) \simeq \hat{\mathbb{Z}} \times U(k).$$

我们可以将所得结果作一个简单的总结. 设 k_{ab} 是局部域 k 的极大 Abel 扩域, 则存在着从 k 的乘法群 k^\times 到 Galois 群 $\mathrm{Gal}(k_{ab}/k)$ 的连续单同态, 叫作基本映射:

$$\rho_k: k^\times \rightarrow \mathrm{Gal}(k_{ab}/k).$$

并且 ρ_k 以自然地(函子地)方式依赖于基域 k . 然后由 ρ_k 得到关于 k 的(有限) Abel 扩域的各种重要定理. 这些是局部类域论的骨干. 今后在第八章我们将考查一个特例, 即 k 为 p -adic 域 \mathbb{Q}_p 的情形. 利用下一章的定理可以得到关于 ρ_k 的一些更具体的结果.

第七章 形式群及其应用

本章中我们引述 Lubin-Tate [9] 中对于局部域的形式群及其应用¹⁾。主要目的在于给出前章存在定理(定理 10)的另一个证明, 用这种方法也可同时得到与基本映射 ρ_x 有关的一些重要结果。

§ 7.1 一般的形式群

开始先简单介绍一下今后需要的关于形式群的知识。详情请参见 Fröblich [4]。

一般地, 设 R 是带 1 交换环。以 $R[[X]]$ 表示系数属于 R 的关于未定元 X 的形式幂级数

$$\sum_{n=0}^{\infty} a_n X^n, \quad a_n \in R$$

全体所构成的集合, 它也是交换环。类似地定义多个未定元的幂级数环 $R[[X, Y]]$, $R[[X, Y, Z]]$ 等。如果 $R[[X]]$ 中的幂级数 $f(X)$, $g(X)$ 没有常数项, 即 $f(0) = g(0) = 0$, 则 $f(g(X))$ 也是没有常数项的幂级数。将这个幂级数记成 $f \circ g$:

$$(f \circ g)(X) = f(g(X)).$$

对于这样的乘法, X 是单位元素。所以如果

$$(f \circ g)(X) = (g \circ f)(X) = X,$$

则 $f = g^{-1}$, $g = f^{-1}$ 。幂级数 $f(X)$ 具有逆元素 f^{-1} 的充要条件是 X 的系数为 R 中可逆元素。

如果 $R[[X, Y]]$ 中幂级数 $F(X, Y)$ 满足如下诸条件, 则

1) 参见 Cassels-Fröblich [3], 第六章, § 3, Serre 的文章。文章中我们沿用 Serre 的记号。

称 F 是 R 上的形式群 (或者更正确地称作是 r -元交换形式群):

- i) $F(X, Y) = X + Y \bmod \deg z$;
- ii) $F(F(X, Y), Z) = F(X, F(Y, Z))$;
- iii) $F(X, Y) = F(Y, X)$.

其中 i) 的意思是: 去掉次数 ≥ 2 的诸项之后, 等式两边的幂级数一样. 从 i) 可知, 关于 X 的幂级数 $F(X, 0)$ 具有逆元素. 在 ii) 中令 $Y = Z = 0$, 则 $F(F(X, 0), 0) = F(X, 0)$, 从而由上面的注记即知

$$F(X, 0) = X.$$

再由 iii) 得出 $F(0, Y) = Y$, 最后得到

$$F(X, Y) = X + Y + \sum_{i,j=1}^{\infty} a_{ij} X^i Y^j, \quad a_{ij} = a_{ji} \in R.$$

如果 $F(X, Y), G(X, Y)$ 均是 R 上的形式群, $f(X)$ 为 $R[[X]]$ 中的幂级数并且 $f(0) = 0$, 如果

$$f(F(X, Y)) = G(f(X), f(Y)),$$

便将 f 叫作是从 F 到 G 的同态, 并且表示成

$$f: F \rightarrow G.$$

如果 f 有可逆元素 f^{-1} , 则 f^{-1} 是从 G 到 F 的同态. 这时将 f 叫作从 F 到 G 的同构, 并且记成

$$f: F \cong G.$$

我们用 $\text{Hom}_R(F, G)$ 表示从 F 到 G 的同态全体. 当 $F = G$ 时, 则将 $\text{Hom}_R(F, F)$ 记成 $\text{End}_R(F)$. 如果 $f, g \in \text{Hom}_R(F, G)$, 则由

$$(f \oplus g)(X) = G(f(X), g(X))$$

定义的 $f \oplus g$ 也属于 $\text{Hom}_R(F, G)$, 并且 $\text{Hom}_R(F, G)$ 对于此加法运算形成 Abel 群. 而 $\text{End}_R(F)$ 对于这一加法和早先定义的乘法 $f \circ g$ 形成环, 其单位元素是幂级数 X .

§ 7.2 形式群 $F_r(X, Y)$

以下与前章一样, 令 k 是局部域, v 为 k 的完备正规赋值,

$$\mathfrak{o}, \mathfrak{p}, \mathfrak{k} = \mathfrak{o}/\mathfrak{p}$$

分别为 k 的 (即 ν 的) 赋值环, 极大理想和剩余类域. 又设有限域 \mathfrak{k} 的元素个数为 q , k 的乘法群 k^\times 的子群 $U_n, n \geq 0$ 定义为

$$U_0 = U = k \text{ 的单位群, } U_n = 1 + \mathfrak{p}^n \quad (n \geq 1).$$

固定 k 的一个素元 π . 以 \mathfrak{S}_π 表示 $\mathfrak{o}[[X]]$ 中满足以下两个同余式的全部元素 $f(X)$ 构成的集合:

$$f(X) \equiv \pi X \pmod{\deg 2}, \quad f(X) \equiv X^q \pmod{\mathfrak{p}}.$$

其中后一个同余式的意思是: $f(X) - X^q$ 的所有系数均属于 \mathfrak{p} .

引理 1 设 $f(X), g(X)$ 均是 \mathfrak{S}_π 中的幂级数, 而线性型

$$a_1 X_1 + \cdots + a_n X_n$$

的系数属于 \mathfrak{o} , 则存在唯一的幂级数

$$F(X_1, \cdots, X_n) \in \mathfrak{o}[[X_1, \cdots, X_n]],$$

使得

$$F(X_1, \cdots, X_n) \equiv a_1 X_1 + \cdots + a_n X_n \pmod{\deg 2},$$

$$f(F(X_1, \cdots, X_n)) = F(g(X_1), \cdots, g(X_n)).$$

证明 令 $F_1 = a_1 X_1 + \cdots + a_n X_n$. 下面我们归纳决定多项式 $F_1, F_2, \cdots, F_n \in \mathfrak{o}[[X_1, \cdots, X_n]]$ 使得满足如下条件:

$$F_n \equiv F_{n-1} \pmod{\deg n},$$

$$f(F_n(X_1, \cdots, X_n)) \equiv F_n(g(X_1), \cdots, g(X_n)) \pmod{\deg n + 1}.$$

为了证明这是可能的, 假设 $n \geq 2$, 并且已经定义了 $F_1, F_2, \cdots, F_{n-1}$. 对于 $\mathfrak{o}[[X_1, \cdots, X_n]]$ 的任意 n 次齐次多项式 G , 令

$$F_n = F_{n-1} + G,$$

则 F_n 满足第一个条件. 由 $f(X) \equiv \pi X, g(X) \equiv \pi X \pmod{\deg 2}$ 可知

$$f(F_n) = f(F_{n-1} + G) = f(F_{n-1})$$

$$+ \pi G \pmod{\deg n + 1},$$

$$F_n(g(X_1), \cdots, g(X_n)) = F_{n-1}(g(X_1), \cdots, g(X_n))$$

$$+ G(g(X_1), \cdots, g(X_n))$$

$$\equiv F_{n-1}(g(X_1), \cdots, g(X_n))$$

$$+ \pi^n G(X_1, \dots, X_n) \bmod \deg n + 1,$$

从而为了满足第二条件,其充要条件是

$$\begin{aligned} f(F_{n-1}) &= F_{n-1}(g(X_1), \dots, g(X_n)) \\ &\equiv \pi(\pi^{n-1} - 1)G \bmod \deg n + 1, \end{aligned} \quad (*)$$

由归纳假设知道左边 $\equiv 0 \bmod \deg n$. 又由于 $n \geq 2$, 从而

$$\pi^n - 1 \in U(k).$$

因此若

$$f(F_{n-1}) = F_{n-1}(g(X_1), \dots, g(X_n)) \bmod p,$$

则存在唯一的 n 次齐次多项式 $G \in \mathfrak{o}[X_1, \dots, X_n]$ 满足同余式 (*). 由于 $f(X) = X^q \bmod p$, $g(X) = X^q \bmod p$, 并且 q 是 p 的幂, 其中 p 是 $\mathfrak{f} = \mathfrak{o}/p$ 的特征, 从而

$$\begin{aligned} f(F_{n-1}) &\equiv F_{n-1}^q \bmod p, \\ F_{n-1}(g(X_1), \dots, g(X_n)) \\ &= F_{n-1}(X_1^q, \dots, X_n^q) \equiv F_{n-1}^q \bmod p. \end{aligned}$$

于是 $F_n = F_{n-1} + G$ 满足定义中的条件, 这就归纳证明了全部 $F_n (n \geq 1)$ 的存在性.

由于 $F_n \equiv F_{n-1} \bmod \deg n$, 从而存在幂级数 $F(X_1, \dots, X_n) \in \mathfrak{o}[[X_1, \dots, X_n]]$, 使得对于每个 $n \geq 1$ 均满足

$$F \equiv F_n \bmod \deg n,$$

这个 F 显然满足引理中的条件. 而且从上面的证明知道 G 是唯一确定的, 从而 F 也是唯一的. 事实上, 基于同样的理由, 满足引理条件的 F 在 $k[[X_1, \dots, X_n]]$ 中也是唯一存在的.

注记 在证明上面引理的时候, 从而在应用于下面的引理 2 和引理 3 的时候, 均不需要 k 的赋值 v 的完备性.

引理 2 设 $f(X)$ 是属于 \mathfrak{F}_k 的幂级数, 则在 \mathfrak{o} 上存在唯一的形式群 $F(X, Y)$ 使得

$$f(X) \in \text{End}_{\mathfrak{o}}(F).$$

证明 根据引理 1 可知存在唯一的幂级数

$$F(X, Y) \in \mathfrak{o}[[X, Y]]$$

满足

$$F(X, Y) \equiv X + Y \pmod{\deg 2},$$

$$f(F(X, Y)) = F(f(X), f(Y)).$$

但是 $F(Y, X)$ 也满足同样的条件, 从而由唯一性可知

$$F(X, Y) = F(Y, X).$$

又在引理 1 中令 $f(X) = g(X)$, 线性型取为 $X + Y + Z$, 则幂级数 $F(F(X, Y), Z)$ 和 $F(X, F(Y, Z)) \in \mathfrak{o}[[X, Y, Z]]$ 均满足引理 1 中的条件, 再由唯一性即知

$$F(F(X, Y), Z) = F(X, F(Y, Z)).$$

因此 $F(X, Y)$ 是 \mathfrak{o} 上的形式群, 并且 $f(X) \in \text{End}_{\mathfrak{o}}(F)$, 由引理 1 证明末尾的注记, 可知 $F(X, Y)$ 在 $k[[X, Y]]$ 中也是唯一存在的.

今将引理 2 中的形式群 $F(X, Y)$ 写成

$$F_f = F_f(X, Y).$$

引理 3 如果 $f(X), g(X) \in \mathfrak{F}_n$, 则对于每个元素 $a \in \mathfrak{o}$, 存在唯一的幂级数 $\phi(X) \in \mathfrak{o}[[X]]$ 满足

$$f \circ \phi = \phi \circ g, \phi(X) \equiv aX \pmod{\deg 2}.$$

如果将这个 $\phi(X)$ 记成 $[a]_{f,g}$, 则

- i) $[a]_{f,g} \in \text{Hom}_{\mathfrak{o}}(F_g, F_f), a \in \mathfrak{o}$;
- ii) $[a]_{f,g} \oplus [b]_{f,g} = [a + b]_{f,g}, a, b \in \mathfrak{o}$;
- iii) $[a]_{f,g} \circ [b]_{g,h} = [ab]_{f,h}, h(X) \in \mathfrak{F}_n, a, b \in \mathfrak{o}$.

证明 由引理 1 立刻得到 $\phi(X)$ 的存在性和唯一性. 令

$$\phi(X) = [a]_{f,g},$$

则 $\phi(F_g(X, Y))$ 和 $F_f(\phi(X), \phi(Y))$ 均是

$$H(X, Y) \equiv a(X + Y) \pmod{\deg 2},$$

$$f(H(X, Y)) = H(g(X), g(Y))$$

的解 H , 但是由引理 1 可知解是唯一的, 从而

$$\phi(F_g(X, Y)) = F_f(\phi(X), \phi(Y)).$$

即

$$[a]_{f,g} \in \text{Hom}_{\mathfrak{o}}(F_g, F_f).$$

其次, ii) 式两边均满足 $f \circ \phi = \phi \circ g$, 并且

$[a]_{f,g} \oplus [b]_{f,g} = [a+b]_{f,g} = (a+b)X \bmod \deg 2$,
因此两者一致. 同样地证明 (ii).

如果 $f(X) = g(X)$, 我们把 $[a]_{f,f}$ 简记成 $[a]_f$:

$$[a]_f = [a]_{f,f}, \quad a \in \mathfrak{o}.$$

由于 $f(X) \in \mathfrak{F}_\pi$, 从 $[a]_f$ 的定义即知

$$[\pi]_f = f(X).$$

此外, 由引理 3 可知 $a \mapsto [a]_f$ 给出环的单同态¹⁾

$$\mathfrak{o} \rightarrow \text{End}_\sigma(F_f).$$

在一般情形下, 对于 $f(X), g(X) \in \mathfrak{F}_\pi$, 则

$$[1]_f = X, \quad [1]_{g,f} = [1]_{f,f},$$

也就是说, 对于固定的素元 π , 对应于 $f(X) \in \mathfrak{F}_\pi$ 的形式群 $F_f(X, Y)$ 彼此是 σ -同构的. 下面再考查对于 k 中不同的素元 π 和 π' , 对应于 $f \in \mathfrak{F}_\pi$ 的形式群 $F_f(X, Y)$ 和对应于 $g(X) \in \mathfrak{F}_{\pi'}$ 的形式群 $F_g(X, Y)$ 之间的关系.

以下仍设 $K = k_{ur}$ 是 k 的极大不分歧扩域, \bar{K} 是 K 的完备化, \mathfrak{o}_K 和 $\mathfrak{o}_{\bar{K}}$ 分别是 K 和 \bar{K} 的赋值环, φ 是 K/k 的 Frobenius 自同构, φ 到 \bar{K} 上的扩充仍记为 φ . 如果 $\omega(X)$ 是 $\mathfrak{o}_K[[X]]$ 或者 $\mathfrak{o}_{\bar{K}}[[X]]$ 中的幂级数, 我们以 $\omega^\varphi(X)$ 表示 $\omega(X)$ 的诸系数 α 改成 $\varphi(\alpha)$ ($= \alpha^q$) 之后所得到的幂级数.

引理 4 假设 $h(X) \in \mathfrak{o}[[X]]$, 并且 $h(X)$ 具有前节意义下的逆元素, 则存在幂级数 $\omega(X) \in \mathfrak{o}_{\bar{K}}[[X]]$, 使得 $\omega(X)$ 可逆并且满足

$$\omega^\varphi = \omega \circ h.$$

证明 我们证明在 $\mathfrak{o}_{\bar{K}}[[X]]$ 中存在多项式序列 $\{\omega_n\}_{n \geq 1}$, 使得

$$\omega_n \equiv \omega_{n+1} \bmod \deg n + 1,$$

$$\omega_n^\varphi \equiv \omega_n \circ h \bmod \deg n + 1, \quad n \geq 1.$$

如果可以证明这件事, 取 $\omega_n (n \geq 1)$ 的极限, 则由第一条条件给出

1) 如果 k 的特征是 0, 则这个映射也是满射. 参见 Frohlich [4], 第四章.

$\mathfrak{o}_K[[X]]$ 中幂级数 $\omega(X)$. 再由第二条件给出 $\omega^\varphi = \omega \circ h$.

由于 $h^{-1} \in \mathfrak{o}[[X]]$, 可知

$$h(X) \equiv uX \pmod{\deg 2}, \quad u \in U(k) \subset U(\bar{K}).$$

其中 $U(k)$ 和 $U(\bar{K})$ 分别是 k 和 \bar{K} 的单位群. 由 § 4.2, 定理 2 可知存在 $\xi_1 \in U(\bar{K})$ 使得

$$u = \xi_1^{\varphi^{-1}}.$$

取

$$\omega_1(X) = \xi_1 X,$$

则

$$\omega_1^\varphi(X) = \xi_1^\varphi X = \xi_1 u X \equiv \omega_1 \circ h(X) \pmod{\deg 2}.$$

现在归纳假设 $\omega_1, \dots, \omega_{n-1}$ ($n \geq 2$) 满足条件, 则存在适当的 $\alpha \in \mathfrak{o}_K$, 使得

$$\omega_{n-1}^\varphi \equiv \omega_{n-1} \circ h + \alpha X^n \pmod{\deg n+1}.$$

对于 \mathfrak{o}_K 中任意元素 ξ_n , 令

$$\omega_n = \omega_{n-1} + \xi_n X^n,$$

则显然 $\omega_n \equiv \omega_{n-1} \pmod{\deg n}$, 并且

$$\omega_n^\varphi = \omega_{n-1}^\varphi + \xi_n^\varphi X^n \equiv \omega_{n-1} \circ h + \xi_n u^n X^n \pmod{\deg n+1},$$

$$\omega_n \circ h = \omega_{n-1} \circ h + \xi_n h^n \equiv \omega_{n-1} \circ h + \xi_n u^n X^n \pmod{\deg n+1}.$$

所以, 为了得到 $\omega_n^\varphi \equiv \omega_n \circ h \pmod{\deg n+1}$, 只需要有

$$\alpha + \xi_n^\varphi = \xi_n u^n$$

即可. 令 $\eta = \xi_n \xi_1^n$, 由于 $u = \xi_1^{\varphi^{-1}}$, 可知上面关于 ξ_n 的等式等价于

$$\eta^\varphi - \eta = -\alpha(u\xi_1)^{-n}.$$

但是右边为 \mathfrak{o}_K 中已知元素, 再由 § 4.2, 定理 2 即知存在 $\eta \in \mathfrak{o}_K$ 满足上式, 于是定义 $\xi_n = \eta \xi_1^n$, 则 $\omega_n = \omega_{n-1} + \xi_n X^n$ 满足

$$\omega_n \equiv \omega_{n-1} \pmod{\deg n}$$

和 $\omega_n^\varphi \equiv \omega_n \circ h \pmod{\deg n+1}$. 这就证明了 $\{\omega_n\}_{n \geq 1}$ 的存在性.

令 ω 是 ω_n 的极限, 则如上所述便有 $\omega^\varphi = \omega \circ h$, 由于

$$\omega \equiv \omega_1 = uX \pmod{\deg 2}, \quad u \in U(\bar{K}),$$

所以存在逆元素 $\omega^{-1} \in \mathfrak{o}_K[[X]]$. 这就证明了引理.

设 π, π' 均是 k 的素元, 则

$$\pi' = u\pi, \quad u \in U.$$

对于幂级数 $f \in \mathfrak{F}_\pi$, 由引理 3 知道 $[u]_f^{-1} = [u^{-1}]_f, u^{-1} \in \mathfrak{o}$, 从而 $[u]_f$ 在 $\mathfrak{o}[[X]]$ 中存在逆元素, 再由引理 4 即知存在

$$\omega(X) \in \mathfrak{o}_K[[X]]$$

满足 $\omega^\varphi = \omega \circ [u]_f$, 并且 $\omega(X)$ 具有逆元素 ω^{-1} . 一般地, 对于任意幂级数 $F(X_1, \dots, X_n) \in \mathfrak{o}_K[[X_1, \dots, X_n]]$, 定义幂级数

$$F^\omega(X_1, \dots, X_n) = \omega(F(\omega^{-1}(X_1), \dots, \omega^{-1}(X_n))),$$

则有如下的引理.

引理 5 令 $g = [\pi']_f^\omega$, 则 $g(X) \in \mathfrak{F}_{\pi'}$ 并且

$$F_g = F_f^\omega, \quad [a]_g = [a]_f^\omega, \quad a \in \mathfrak{o}.$$

证明 根据定义可知 $[a]_f^\omega = \omega \circ [a]_f \circ \omega^{-1}$, 注意 $[a]$ 是 $\mathfrak{o}[[X]]$ 中的幂级数, 因此

$$\begin{aligned} ([a]_f^\omega)^\varphi &= \omega^\varphi \circ [a]_f \circ (\omega^{-1})^\varphi = \omega \circ [u]_f \circ [a]_f \circ [u]_f^{-1} \circ \omega^{-1} \\ &= \omega \circ [a]_f \circ \omega^{-1} = [a]_f^\omega. \end{aligned}$$

从而由 § 4.2, 定理 2 即知 $[a]_f^\omega \in \mathfrak{o}[[X]]$. 又显然有

$$[a]_f^\omega \equiv [a]_f \equiv aX \pmod{\deg 2}, \quad a \in \mathfrak{o}.$$

特别取 $a = \pi'$, 则

$$g = [\pi']_f^\omega \in \mathfrak{o}[[X]], \quad g(X) \equiv \pi'X \pmod{\deg 2}.$$

另一方面, Frobenius 自同构 φ 诱导出剩余类域 $\mathfrak{f}_K = \mathfrak{f}_{\bar{K}} = \mathfrak{o}_{\bar{K}}/\mathfrak{p}_{\bar{K}}$ 上的自同构 $\kappa \mapsto \kappa^q$, 其中 q 为 $\mathfrak{f}_{\bar{K}}$ 的特征的幂, 从而

$$\omega^\varphi \circ X^q = \omega^\varphi(X^q) \equiv \omega(X)^q \pmod{\mathfrak{p}_{\bar{K}}}.$$

再注意 $[\pi']_f = [u]_f \circ [\pi]_f$, $[\pi]_f \equiv X^q \pmod{\mathfrak{p}}$, 因此

$$\begin{aligned} g &= \omega \circ [u]_f \circ [\pi]_f \circ \omega^{-1} = \omega^\varphi \circ [\pi]_f \circ \omega^{-1} = \omega^\varphi \circ X^q \circ \omega^{-1} \\ &\equiv \omega^q \circ \omega^{-1} \equiv X^q \pmod{\mathfrak{p}_{\bar{K}}}. \end{aligned}$$

即 $g \equiv X^q \pmod{\mathfrak{p}}$. 从而 $g \in \mathfrak{F}_{\pi'}$. 进而,

$$\begin{aligned} (F_f^\omega)^\varphi &= \omega^\varphi \circ F_f((\omega^\varphi)^{-1}(X), (\omega^\varphi)^{-1}(Y)) \\ &= \omega \circ [u]_f \circ F_f([u]_f^{-1} \circ \omega^{-1}(X), [u]_f^{-1} \circ \omega^{-1}(Y)) \\ &= \omega \circ F_f(\omega^{-1}(X), \omega^{-1}(Y)) = F_f^\omega. \end{aligned}$$

这里用到了 $[u]_f \in \text{End}_*(F_f)$. 再注意到

$$o_K[[X, Y]] = (o_K[[X]])[[Y]],$$

由 § 4.2, 定理 2 即知 $F_f^\pi \in o[[X, Y]]$. 由 $[\pi]_f \in \text{End}_o(F_f)$ 不难得到 $g = [\pi']_f \in \text{End}_o(F_f^\pi)$, 这就证明了 $F_g = F_f^\pi$. 最后由

$$[a]_f \circ [\pi']_f = [\pi']_f \circ [a]_f$$

可知

$$[a]_f^\pi \circ g = g \circ [a]_f^\pi, \quad a \in o.$$

由于 $[a]_f^\pi \in o[[X]]$, $[a]_f^\pi = aX \bmod \deg 2$, 再由定义即知

$$[a]_f^\pi = [a]_g.$$

从上面的引理以及早先的注记可知, 对于任意的 $f \in \mathfrak{F}_\pi$, $g \in \mathfrak{F}_{\pi'}$ (即使在 $\pi \approx \pi'$ 的时候), $F_f(X, Y)$ 和 $F_g(X, Y)$ 作为 o_K 上的形式群是同构的.

§ 7.3 Abel 扩域 k_{π^*} .

如前章一样, 取 \mathcal{O} 为 k 的代数闭包, $\bar{\mathcal{O}}$ 是 \mathcal{O} 的完备化. 为简单起见, 今后用 \mathfrak{m} 表示 $\bar{\mathcal{O}}$ 对于赋值 μ 的极大理想 $\mathfrak{p}_{\bar{\mathcal{O}}}$:

$$\mathfrak{m} = \mathfrak{p}_{\bar{\mathcal{O}}} = \{\alpha \in \bar{\mathcal{O}} \mid \mu(\alpha) = 0\}.$$

固定 k 的素元 π 和 \mathfrak{F}_π 中一个幂级数 $f(X)$, 则形式群 $F_f(X, Y)$ 属于 $o[[X, Y]]$. 由于 $\bar{\mathcal{O}}$ 是完备的, 可知对于任意元素 $\alpha, \beta \in \mathfrak{m}$, $F_f(\alpha, \beta)$ 在 $o_{\bar{\mathcal{O}}}$ 中收敛. 又因为 $F_f(0, 0) = 0$, 从而 $F_f(\alpha, \beta)$ 也属于 \mathfrak{m} . 我们令

$$\alpha \dot{+} \beta = F_f(\alpha, \beta).$$

从形式群的定义可知 \mathfrak{m} 对于这一加法运算形成 Abel 群. 以后将此群记成 \mathfrak{m}_f . 由于 $F(X, 0) = X$ 可知 0 是 \mathfrak{m}_f 中零元素. 进而, 由于 $[a]_f \in \text{End}_o(F_f)$,

$$[a]_f(\alpha \dot{+} \beta) = [a]_f(\alpha) \dot{+} [a]_f(\beta), \quad \alpha, \beta \in \mathfrak{m}_f.$$

从而由

$$\begin{aligned} o \times \mathfrak{m}_f &\rightarrow \mathfrak{m}_f \\ (a \times \alpha) &\mapsto [a]_f(\alpha) \end{aligned}$$

使 \mathfrak{m}_f 成为 o -模 (参见引理 3 的 ii) 和 iii)). 今后在不发生混淆

的时候,我们将 $[a](\alpha)$ 简记为 $a \cdot \alpha$.

对于每个 $n \geq 0$, 令

$$\begin{aligned} E_f^n &= \{\alpha \in m_f \mid p^n \cdot \alpha = 0\} = \{\alpha \in m_f \mid \pi^n \cdot \alpha \\ &= [\pi^n]_f(\alpha) = 0\}. \end{aligned}$$

(注意 $p^n = \pi^n$). 显然 E_f^n 是 m_f 的 \mathfrak{o} -子模, 并且

$$0 = E_f^0 \subseteq E_f^1 \subseteq \cdots \subseteq E_f^n \subseteq \cdots \subseteq m_f.$$

从而

$$E_f = \bigcup_{n \geq 0} E_f^n$$

也是 m_f 的 \mathfrak{o} 子模, 它显然是 \mathfrak{o} -模 m_f 的扭 (torsion) 子模.

如果 $g(X)$ 为 \mathfrak{F}_π 中另一个幂级数, 则

$$[1]_{f,g}: F_g \xrightarrow{\sim} F_f, [a]_{f,g} \in \text{Hom}_{\mathfrak{o}}(F_g, F_f), a \in \mathfrak{o},$$

从而由

$$\begin{aligned} [1]_{f,g}: m_g &\xrightarrow{\sim} m_f \\ \alpha &\longmapsto [1]_{f,g}(\alpha) \end{aligned}$$

给出从 m_g 到 m_f 的 \mathfrak{o} 同构. 并且由此同构可知

$$[1]_{f,g}(E_g^n) = E_f^n, [1]_{f,g}(E_g) = E_f, \quad n \geq 0.$$

根据定义可知 \mathfrak{F}_π 中包含多项式

$$g(X) = X^q + \pi X.$$

现在我们来研究对于这个 $g(X)$ 的 \mathfrak{o} 模 E_g^n . 对于每个 $n \geq 0$, 将 $g(X)$ 自乘 n 次的乘积记为

$$g^{(n)}(X) = g \circ g \circ \cdots \circ g(X).$$

由定义可知

$$g^{(0)}(X) = X,$$

$$g^{(n)}(X) = g(g^{(n-1)}(X)) = (g^{(n-1)}(X)^q + \pi)g^{(n-1)}(X),$$

$$n \geq 1.$$

因此当 $n \geq 1$ 时若令

$$h^{(n)}(X) = g^{(n-1)}(X)^{q-1} + \pi,$$

则 $g^{(n)}(X), h^{(n)}(X) \in \mathfrak{o}_f[X]$ 并且显然有

$$g^{(n)}(X) = X^{q^n} + \cdots + \pi^n X \equiv X^{q^n} \pmod{p},$$

$$\begin{aligned} h^{(n)}(X) &= X^{(q-1)q^{n-1}} + \dots + x^{(q-1)(q-1)}X^{q-1} + x \\ &\equiv X^{(q-1)q^{n-1}} \pmod{p}, \end{aligned}$$

$$g^{(n)}(X) = h^{(n)}(X)h^{(n-1)}(X)\cdots h^{(1)}(X)X.$$

特别地, $h^{(n)}(X)$ ($n \geq 1$) 是 $(q-1)q^{n-1}$ 次的 Eisenstein 多项式, 因此在 $k[X]$ 中不可约. 如果 k 的特征为 p , 则 q 为 p 的幂, 这时导函数 $dh^{(n)}/dX$ 中 X^{q-2} 的系数 $n^{(n-1)(q-1)}(q-1)$ 不为零. 所以在任何情形下 $h^{(n)}(X)$ 均是可分的不可约多项式. 而 $g^{(n)}(X)$ 是次数相异的不可约多项式之积, 从而也是 $k[X]$ 中可分多项式, 因此它在 k 的代数闭包 Ω 中恰好有 q^n 个不同的根. 由于

$$[\pi]_g = g, [\pi^n]_g = [\pi]_g \circ \cdots \circ [\pi]_g = g^{(n)}(X),$$

从而由定义即知

$$E_g^n = \{\alpha \in m_g \mid g^{(n)}(\alpha) = 0\}.$$

如果 $\alpha \in \Omega$ 或者 $\alpha \in \bar{\Omega}$ 使得 $g^{(n)}(\alpha) = 0$, 则由

$$g^{(n)}(X) \equiv X^{q^n} \pmod{p}$$

可知 $\alpha \in p_{\bar{\Omega}} = m_g$. 因此

$$E_g^n = \{\alpha \in \Omega \mid g^{(n)}(\alpha) = 0\}. \quad (1)$$

换句话说, E_g^n 由 $g^{(n)}(X)$ 在 Ω 中的全部根所组成的集合, 根据上面所述, 它恰好是由 q^n 个元素组成的 \mathfrak{o} -模.

现在考虑一般的 $f(X) \in \mathfrak{F}_x$. 假设 f, g 均属于 \mathfrak{F}_x , 在 \mathfrak{o} -同构 $[1]_{f,g}: m_g \xrightarrow{\sim} m_f$ 之下我们有 $[1]_{f,g}(E_g^n) = E_f^n$, 因此由上面所述可知对于一般的 $f(X)$ 来说, E_f^n 均是由 q^n 个元素组成的 \mathfrak{o} -模. 从而当 $n \geq 1$ 时, $E_f^n \cong E_f^{n-1}$. 如果取定一个元素

$$\alpha \in E_f^n - E_f^{n-1},$$

并且定义 \mathfrak{o} -模同态

$$\mathfrak{o} \rightarrow E_f^n, \quad a \mapsto a \cdot \alpha,$$

由于 $p^n \alpha = 0$, $p^{n-1} \alpha \neq 0$, 从而这个同态的核是 p^n . 因为 \mathfrak{o} 中非零理想均是 p 的幂 p^n ($n \geq 0$), 并且 $[\mathfrak{o}; p^n] = q^n$, 从而上面的同态诱导出 \mathfrak{o} -模同构

$$\mathfrak{o}/p^n \xrightarrow{\sim} E_f^n. \quad (2)$$

对于每个 $a \in \mathfrak{o}$, 定义 \mathfrak{o} -模 E_f^n ($n \geq 0$) 的自同态

$$[a]_f: E_f^n \rightarrow E_f^n,$$

然后由 $a \mapsto [a]_f$ 得到环同态

$$\sigma \rightarrow \text{End}_\sigma(E_f^n).$$

引理 6 上面的映射诱导出自然同构

$$\sigma/\mathfrak{p}^n \cong \text{End}_\sigma(E_f^n), \quad U/U_n \cong \text{Aut}_\sigma(E_f^n).$$

其中 $\text{Aut}_\sigma(E_f^n)$ 是 E_f^n 的 σ -自同构群.

证明 上面给出了 σ -模同构 $E_f^n \cong \sigma/\mathfrak{p}^n (n \geq 1)$. 然后再由环同态 $\sigma \rightarrow \text{End}_\sigma(E_f^n)$ 即得到环同构 $\sigma/\mathfrak{p}^n \cong \text{End}_\sigma(E_f^n)$. 这对于 $n = 0$, $E_f^0 = 0$ 的情形也是对的. 如果将有限环 σ/\mathfrak{p}^n 的乘法群等同于 U/U_n , 又由于 $\text{End}_\sigma(E_f^n)$ 的乘法群是 $\text{Aut}_\sigma(E_f^n)$, 就得到引理中第二个乘法群的同构.

注记 我们一开始定义的 σ -模同构 $\sigma/\mathfrak{p}^n \cong E_f^n$ 依赖于元素 $\alpha \in E_f^n \rightarrow E_f^{n-1}$ 的选取方式, 但是上一引理的同构均是自然的同构.

如上令 $f(X)$ 为 \mathfrak{F}_n 中任意幂级数, 由定义知道 $E_f^n \subset \mathfrak{m}_f \subset \bar{\mathcal{O}}$, 从而 $k(E_f^n)$ 是 $\bar{\mathcal{O}}/k$ 的中间域. 特别对于 $g(X) = X^n + \pi X$, 由(1)式可知 $k(E_g^n)$ 是可分多项式 $g^{(n)}(X)$ 在 k 上的分裂域, 于是 $k(E_g^n)/k$ 为有限 Galois 扩张, 从而 $k(E_g^n)$ 也是局部域. 由于 $[1]_{f,g}(X)$ 是 $\sigma[[X]]$ 中的幂级数, 如果 α 属于局部域 $k(E_g^n)$ 的极大理想, 则 $[1]_{f,g}(\alpha)$ 在 $k(E_f^n)$ 中收敛. 因此

$$E_f^n = [1]_{f,g}(E_g^n) \subset k(E_g^n), \quad k \subseteq k(E_f^n) \subseteq k(E_g^n).$$

从而 $k(E_f^n)$ 也是局部域. 从而又与上面同样地得到

$$E_g^n = [1]_{g,f}(E_f^n) \subseteq k(E_f^n), \quad k \subseteq k(E_g^n) \subseteq k(E_f^n),$$

从而

$$k(E_f^n) = k(E_g^n).$$

换句话说, 对于 \mathfrak{F}_n 中每个 $f(X)$, $k(E_f^n)$ 是同一个域. 今后将这个域记成 k_f^n :

$$k_f^n = k(E_f^n), \quad f \in \mathfrak{F}_n, \quad n \geq 0.$$

特别有

$$k_f^0 = k(0) = k.$$

设 π' 是 k 的另一个素元, 则

$$\pi' = \pi u, \quad u \in U.$$

如果 $K = k_{ur}$, 而 φ 是 K/k 的 Frobenius 自同构, 则由引理 4 和 5 可知存在幂级数 $\omega(X) \in \mathfrak{o}_K[[X]]$ 使得

$$\omega^\varphi = \omega \circ [u]_f.$$

由于

$$f(X) = [\pi']_f^\omega(x) \in \mathfrak{F}_{\pi'},$$

并且对于每个 $a \in \mathfrak{o}$,

$$[a]_{f'} = [a]_f^\omega = \omega \circ [a]_f \circ \omega^{-1}.$$

从而由 E_f^π 和 $E_{f'}^\pi$ 的定义有

$$E_{f'}^\pi = \omega(E_f^\pi). \quad (3)$$

设 \bar{L}, \bar{L}' 分别为 $L = k_x^\pi K$ 和 $L' = k_{\pi'}^\pi K$ 的完备化. 由引理 5, 6 可知 L 和 L' 分别是 k_x^π 和 $k_{\pi'}^\pi$ 的极大不分歧扩域, 并且

$$\bar{L} = k_x^\pi K = K(E_f^\pi), \quad \bar{L}' = k_{\pi'}^\pi K = K(E_{f'}^\pi).$$

由于 $\omega(X)$ 在 $\mathfrak{o}_K[[X]]$ 中有逆元素, 由 (3) 式即知

$$\bar{L} = \bar{L}'.$$

再由 § 4.3, 引理 6 的系可知

$$L = \bar{L} \cap \mathcal{O}_x = \bar{L}' \cap \mathcal{O}_x = L'.$$

换句话说, 如果令

$$M^n = k_x^\pi k_{ur} = k_x^\pi K,$$

则 M^n 只依赖于 n 而与素元 π 无关. 由以上即知

$$M^n = (k_x^\pi)_{ur}.$$

设 φ' 为 M^n/k_x^π 的 Frobenius 自同构, 并且将 φ' 到 M^n 的完备化 \bar{M}^n 上的扩充仍记为 φ' . 我们马上就要证明 k_x^π/k 完全分歧, 即 $k_x^\pi \cap k_{ur} = k$. 由此可知

$$\varphi'|_K = \varphi, \quad \varphi'|_{\bar{K}} = \varphi.$$

从而对于每个元素 $\alpha \in E_f^\pi$, 令 $\alpha' = \omega(\alpha) \in E_{f'}^\pi$, 则 α 和 α' 均属于 M^n , 并且 $\varphi'(\alpha) = \alpha$, 从而得到

$$\omega(\alpha)^{\varphi'} = \omega^{\varphi'}(\alpha^{\varphi'}) = \omega^\varphi(\alpha) = \omega \circ [u]_f(\alpha). \quad (4)$$

定理 1 设 π 为局部域 k 的任意素元, $n \geq 1$ 为自然数, k_x^π

和 $M^n = k_x^n k_{ur}$ 定义如上, 则 k_x^n/k 是有限完全分歧 Abel 扩张, 从而 M^n/k 也是 Abel 扩张. 并且

$$[k_x^n : k] = [M^n : k_{ur}] = (q-1)q^{n-1},$$

$$N(k_x^n/k) = \langle \pi \rangle \times U_n,$$

$$N(M^n/k) = NU(M^n/k) = NU(k_x^n/k) = U_n.$$

证明 令 $g(X) = X^q + \pi X$, 如上定义 $g^{(n)}(X)$ 和 $h^{(n)}(X)$. 取 $\alpha \in E_g^n - E_g^{n-1}$, 再令

$$k' = k(\alpha), \quad k \subseteq k' \subseteq k_x^n = k(E_g^n).$$

由于 $g^{(n)}(\alpha) = 0$, $g^{(n-1)}(\alpha) \neq 0$, 从而 α 是 $h^{(n)}(X)$ 的根, 但是 $h^{(n)}(X)$ 是 $k[X]$ 中 $(q-1)q^{n-1}$ 次不可约多项式并且常数项是 π , 从而

$$(q-1)q^{n-1} = [k' : k] \leq [k_x^n : k],$$

$$\pi = N_{k'/k}(-\alpha). \quad (5)$$

由 § 1.3, 定理 3 的系即知 k'/k 完全分歧并且 $\pm \alpha$ 是 k' 的素元. 而前面已经证明了 $k_x^n = k(E_g^n)$ 是 k 的有限 Galois 扩域. 另一方面, $F_g(X, Y)$ 和 $[a]_g(X) (a \in \mathfrak{o})$ 均是系数属于 \mathfrak{o} 的幂级数, 从而对于每个元素 $\sigma \in \text{Gal}(k_x^n/k)$ 和 $\beta, \gamma \in E_g^n$ 均有

$$F_g(\beta^\sigma, \gamma^\sigma) = F_g(\beta, \gamma)^\sigma, \quad a \cdot \beta^\sigma = (a \cdot \beta)^\sigma.$$

由于 E_g^n 为 $g(X)$ 的根集合, 从而 $\sigma(E_g^n) = E_g^n$, 所以 σ 诱导出 \mathfrak{o} -模 E_g^n 的自同构 σ' , 而 $\sigma \mapsto \sigma'$ 定义出同态

$$\text{Gal}(k_x^n/k) \rightarrow \text{Aut}_{\mathfrak{o}}(E_g^n).$$

但是 $k_x^n = k(E_g^n)$, 从而这个同态是单射. 于是由引理 6 可知

$$\begin{aligned} [k_x^n : k] &= [\text{Gal}(k_x^n/k) : 1] \leq [\text{Aut}_{\mathfrak{o}}(E_g^n) : 1] \\ &= [U : U_n] = (q-1)q^{n-1}. \end{aligned}$$

从而再由 (5) 便得到

$$k_x^n = k', \quad [k_x^n : k] = (q-1)q^{n-1}, \quad \pi \in N(k_x^n/k),$$

$$\text{Gal}(k_x^n/k) \cong \text{Aut}_{\mathfrak{o}}(E_g^n) \cong U/U_n,$$

从而 k_x^n/k 是完全分歧的 Abel 扩张.

其次对于任意元素 $u \in U_n$, 则 $\pi' = \pi u$ 也是 k 的素元, 则本定理之前面所述结果对于 π' 和 $f = g$ 是适用的. 由 U_n 的定义可

知

$$u = 1 + x, \quad x \in \mathfrak{p}^n,$$

而对于任意元素 $\beta \in E_g^n$, 则有

$$[u]_g(\beta) = [1 + x]_g(\beta) = \beta + x \cdot \beta,$$

由于 $\beta \in E_g^n$, $x \in \mathfrak{p}^n$, 从而 $x \cdot \beta = 0$. 于是 $[u]_g(\beta) = \beta$. 但是上面已经证明了 k_x^n/k 是完全分歧的, 从而由(4)式可知

$$\omega(\beta)^{\varphi'} = \omega \circ [u]_g(\beta) = \omega(\beta).$$

由于 φ' 是 M^n/k_x^n 的 Frobenius 自同构, 从而由上面等式可知

$$\omega(\beta) \in k_x^n.$$

因此

$$E_{g'}^n : \omega(E_g^n) \subseteq k_x^n, \quad k_x^n \subset k_{x'}^n.$$

但是我们已经证明了

$$[k_{x'}^n : k] = [k_x^n : k] \cdot (q - 1)q^{n-1}, \quad \pi' \in N(k_{x'}^n/k),$$

从而得到

$$k_{x'}^n = k_x^n, \quad \pi' \in N(k_x^n/k),$$

由 $\pi' = \pi u$ 和 $\pi \in N(k_x^n/k)$ 又得到 $u \in N(k_x^n/k)$, 但是 u 为 U_n 中任意元素, 从而

$$U_n \subseteq N(k_x^n/k),$$

于是

$$\langle \pi \rangle \times U_n \subseteq N(k_x^n/k). \quad (6)$$

又由于 $k^x = \langle \pi \rangle \times U$, 从而

$$[k^x : \langle \pi \rangle \times U_n] = [U : U_n] = (q - 1)q^{n-1}.$$

另一方面, 对于 Abel 扩张 k_x^n/k 有基本等式

$$[k^x : N(k_x^n/k)] = [k_x^n : k] = (q - 1)q^{n-1}.$$

从而由(6)式即知

$$N(k_x^n/k) = \langle \pi \rangle \times U_n,$$

于是得到

$$NU(k_x^n/k) = U_n.$$

因为 $M^n = k_x^n K$, 由 § 4.3, 引理 5 可知

$$N(M^n/k) = NU(M^n/k) = NU(k_x^n/k) = U_n.$$

这就完全证明了定理.

根据上述定理, 对于 Abel 扩张 M^n/k 有 $N(M^n/k) = U_n$. 但是全部 $U_n (n \geq 1)$ 的交集为 $\{1\}$, 从而

$$N(k_{ab}/k) = 1.$$

这又给出 § 5.3, 定理 2 的另一个证明. 而我们已经说过, 这个 § 5.3, 定理 2 和存在定理 (§ 6.3, 定理 10) 本质上是等价的.

$$N(M^n/k) = U_n$$

是由 $NU(k^n/k) = U_n$ 得到的. 而在证明后者的时候, 除了形式群的有关结果之外, 对于 Abel 扩张 k^n/k 的基本等式也是重要的. 我们在 § 5.1 节末尾说过, 基本等式可以从 § 5.1 中对于有限 Abel 扩张所作的研究直接推导出来. 还参见第五章末尾的注记.

注记 在证明定理 1 的过程中得到同构 $\text{Gal}(k^n/k) \cong U/U_n$, 关于这个同构我们在定理 2 中再作进一步的说明.

定理 2 设 π 是局部域 k 的素元, $f(X)$ 为 \mathbb{S}_π 中任意幂级数. 令 ρ_k 为 k 的基本映射, δ_k 是 § 5.3 中的拓扑同构, 则对于每个 $u \in U$ (k 的单位群) 和 $\alpha \in E_f$, 均有

$$\rho_k(u)(\alpha) = [u^{-1}]_f(\alpha), \quad \delta_k(u)(\alpha) = [u]_f(\alpha).$$

证明 令 $\pi' = \pi u$. 与证明定理 1 一样地, 由引理 4 和 5 可知存在幂级数 $\omega(X) \in \mathbb{O}_K[[X]]$ 使得 $\omega^p = \omega \circ [u]_f$. 于是

$$E_f^p = \omega(E_f^p), \quad f'(X) = [\pi']_f'(X).$$

因此若 $\alpha \in E_f^p$, 则 $\alpha' = \omega(\alpha) \in E_f^p$. 又令

$$\sigma = \rho_k(u), \quad \phi = \rho_k(\pi),$$

$$\phi' = \rho_k(\pi') = \rho_k(\pi)\rho_k(u) = \phi\sigma = \sigma\phi.$$

由定理 1 知道 $\pi \in N(k^n/k)$, 从而由 § 6.2, 定理 5, ii) 可知

$$\rho_k(\pi) \cdot k^n = 1, \quad n \geq 0.$$

但是当 n 充分大时, E_f 中元 α 均属于 $k^n = k(E_f^p)$, 从而

$$\alpha^\psi = \phi(\alpha) = \alpha.$$

同样地 $\alpha'^\psi = \phi'(\alpha') = \alpha'$. 从而

$$\alpha'^\psi = (\alpha')^\sigma = \alpha^\sigma.$$

又由于 $\phi'|_K = \phi|_K = \varphi$, 从而 $\phi'|_K$ 扩充成完备化 \bar{K} 的自同

构 $\varphi(=\bar{\varphi})$. 从而由 $\alpha' = \omega(\alpha)$ 及上述等式得到

$$\begin{aligned}\omega(\alpha) &= \omega(\alpha)^{\varphi'} = \omega^{\varphi}(\alpha^{\varphi'}) = \omega^{\varphi}(\alpha^{\sigma}) \\ &= \omega^{\sigma}([u]_f(\alpha^{\sigma})).\end{aligned}$$

但是 ω 具有逆元素 ω^{-1} . 于是

$$\alpha = [u]_f(\alpha^{\sigma}).$$

从而得到

$$\sigma(\alpha) = \alpha^{\sigma} = [u^{-1}]_f(\alpha), \quad \alpha \in E_f.$$

再由 $\delta_k(u) = \rho_k(u^{-1})$ 即证明了定理 2.

由定理 1 可知 $N(k_n^*/k) = \langle \pi \rangle \times U_n$, 再由 § 6.3, 定理 7 又知 k 的基本映射 ρ_k 诱导出同构

$$\rho_{k'/k}: k^*/N(k_n^*/k) = U/U_n \cong \text{Gal}(k_n^*/k).$$

其中 $k' = k_n^*$. 又由于 $NU(M^*/k) = U_n$, 于是由 § 5.3 可知 δ_k 诱导出同构

$$U/U_n \cong \text{Gal}(M^*/k_{ur}).$$

由于 k_n^*/k 完全分歧, 即 $k_n^* \cap k_{ur} = k$, 从而

$$\text{Gal}(M^*/k_{ur}) = \text{Gal}(k_n^*/k).$$

因此 δ_k 也定义出

$$U/U_n \cong \text{Gal}(k_n^*/k).$$

由定理 2 可知, 这个同构是 $u \bmod U_n \mapsto \sigma$, 其中对于每个 $\alpha \in E_f$,

$$\sigma(\alpha) = [u]_f(\alpha).$$

将此与定理 1 证明中所得到的同构定义

$$\text{Gal}(k_n^*/k) \cong U/U_n$$

相比较, 可知这两个同构是互逆的.

定理 3 对于 Abel 扩张 k_n^*/k , 根据 § 1.4 所述方式定义 Galois 群 $G = \text{Gal}(k_n^*/k)$ 的子群 $G_i (i \geq 0)$, 而令

$$\rho_{k'/k}: U/U_n \cong \text{Gal}(k_n^*/k)$$

是上述同构映射, 又令 $q^{m-1} - 1 < i \leq q^m - 1$, $0 \leq m < n$, 则

$$G_i = \rho_{k'/k}(U_m/U_n) = \text{Gal}(k_n^*/k_m^*).$$

又若 $i \geq q^{n-1}$, 则 $G_i = 1$.

证明 如定理 1 证明中所述, 如果 $\alpha \in E_k^n = E_k^{n-1}$, 则 α 为 k^n 中素元并且 $k^n = k(\alpha)$. 取 $u \in U_m = U_{m+1}$, $0 \leq m < n$, 即

$$u = 1 + x, \quad x \in \mathfrak{p}^m = \mathfrak{p}^{m+1}.$$

又取

$$\sigma = \rho_{k'/k}(u \bmod U_n), \quad \alpha' = [x]_k(\alpha) \quad x = \alpha,$$

则由上定理及 § 7.1 的注记可知

$$\begin{aligned} \sigma(\alpha) &= [u]_k(\alpha) = [1+x]_k(\alpha) \\ &= \alpha + x \cdot \alpha = F_k(\alpha, \alpha') \\ &= \alpha + \alpha' + \sum_{i,j=1}^{\infty} a_{ij} \alpha^i \alpha'^j, \quad a_{ij} = a_{ji} \in \mathfrak{o}. \end{aligned}$$

设 v' 为 $k' = k^n$ 中正规赋值, 由于 $\alpha \in E_k^n \subset \mathfrak{m}_k \cap k'$, 从而

$$v'(\alpha) > 0.$$

于是由上面等式可知

$$v'(\sigma(\alpha) - \alpha) = v'(\alpha').$$

另一方面, 由 $x \in \mathfrak{p}^m = \mathfrak{p}^{m+1}$ 和同构 (2): $\mathfrak{o}/\mathfrak{p}^n \cong E_k^n = \sigma \cdot \alpha$ 可知 $\mathfrak{p}^{n-m} \cdot \alpha' = 0$, $\mathfrak{p}^{n-m-1} \cdot \alpha \neq 0$, 从而

$$\alpha' \in E_k^{n-m} = E_k^{n-m-1}.$$

因此由定理 1 的证明可知 α' 是 k_k^{n-m} 的素元. 但是 k_k^n/k_k^{n-m} 是 q^m 次完全分枝扩张, 因此对于 k_k^{n-m} 的素元 α' 有 $v'(\alpha') = q^m$, 即

$$v'(\sigma(\alpha) - \alpha) = q^m.$$

由 $G_i (i \geq 0)$ 的定义可知当 $u \in U_m = U_{m+1} (0 \leq m < n)$ 时

$$\rho_{k'/k}(u \bmod U_n) \in G \quad (0 \leq i < q^m),$$

$$\rho_{k'/k}(u \bmod U_n) \notin G_{q^m}.$$

由此不难得到, 当 $q^{m-1} - 1 < i \leq q^m - 1 (0 \leq m < n)$ 时

$$G_i = \rho_{k'/k}(U_m/U_n).$$

其次设 $\sigma \in G_i, i \geq q^{n-1}$. 如果 $\sigma = \rho_{k'/k}(u \bmod U_n), u \in U$, 则由上述结果可知必然 $u \in U_n$. 从而 $\sigma = 1$. 于是当 $i \geq q^{n-1}$ 时 $G_i = 1$. 最后由定理 1 即知 $\rho_{k'/k}(U_m/U_n) = \text{Gal}(k_k^n/k_k^m)$.

定理 3 可以推广到 k' 为 k 的任意有限 Abel 扩域的情形. 设 $G = \text{Gal}(k/k)$, 则可以具体地给出 § 1.4 中定义的 G 的子群序列

$G_i (i \geq 0)$ 和用定理 1 中 M^n 所定义的另一子群序列

$$G^i = \text{Gal}(k'/k' \cap M^i), \quad i \geq 0,$$

之间的关系 (Herbrand 定理). 本书不包含这个定理, 因为它需要关于局部域的共轭差积与分歧群的精密结果, 详见 Artin [1] 或者 Serre [11].

又设 π 是局部域 k 中的素元, $f(X) \in \mathfrak{O}_\pi$. 由于

$$E_f^{n-1} \subset E_f^n, \quad k_\pi^n = k(E_f^n),$$

从而

$$k = k_f^0 \subset k_f^1 \subset \cdots \subset k_\pi^n \subset \cdots \subset \mathcal{O}.$$

从而所有 $k_\pi^n (n \geq 0)$ 之并 k_π 也是 k 的 Abel 扩域:

$$k_\pi = \bigcup_{n \geq 0} k_\pi^n = k(E_f), \quad k \subseteq k_\pi \subseteq k_{ab}.$$

由于 $N(k_\pi^n/k) = \langle \pi \rangle \times U_n$, 从而得到

$$N(k_\pi/k) = \langle \pi \rangle.$$

定理 4 设 $\rho_k: k^\times \rightarrow \text{Gal}(k_{ab}/k)$ 是 k 的基本映射, 则 k_π 与 k_{ab} 中的全体 $\rho_k(\pi)$ -不变元素是一致的. 从而由 § 4.3, 引理 7 可知

$$k_{ab} \cap k_\pi = k, \quad k_{ab} k_\pi = k_{ab}.$$

证明 令 $\phi = \rho_k(\pi)$, 并且以 F_ϕ 表示 k_{ab} 中 ϕ -不变元素全体形成的子域 (§ 6.1). 由于 $\pi \in N(k_\pi^n/k)$, 从而由 § 6.3, 定理 7 可知 $\rho_k(\pi) \in \text{Gal}(k_{ab}/k_\pi^n)$, 从而对于每个 $n \geq 0$ 均有

$$\phi|_{k_\pi^n} = \rho_k(\pi)|_{k_\pi^n} = 1.$$

于是 $\phi|_{k_\pi} = 1$, 从而 $k_\pi \subset F_\phi$. 反之, 如果 $k \subset k' \subseteq F_\phi$, $[k':k] < +\infty$, 则 $\phi|_{k'} = 1$, $\phi = \rho_k(\pi)$, 再由 § 6.3, 定理 7 可知

$$\pi \in N(k'/k),$$

从而

$$N(k'/k) = \langle \pi \rangle \times NU(k'/k).$$

由于 $NU(k'/k)$ 是 $U = U(k)$ 的开子群, 而 $\{U_n\}_{n \geq 0}$ 形成 U 中 1 的基本邻域系, 从而当 n 充分大时我们有 $U_n \subseteq NU(k'/k)$. 因此对于这样的 n , 我们有

$$N(k_\pi^n/k) = \langle \pi \rangle \times U_n \subseteq N(k'/k).$$

从而由 § 6.3, 定理 8 有

$$k \subseteq k' \subseteq k_x^* \subseteq k_x.$$

这对于上述每个 k' 均成立, 于是得到 $F_\phi \subseteq k_x$. 从而 $k_x = F_\phi$. 由此及 § 4.3, 引理 7 即得定理后一半.

注记 下面是证明 $k_x = F_\phi$ 的另一种方法, 虽然本质上与前一证明是相同的. 根据 § 6.3 所述, k 的所有有限 Abel 扩域 k' 和 k^* 的所有指数有限的闭子群 H 之间是一一对应的:

$$k' \mapsto H = N(k'/k).$$

这可以扩充成 k 的所有 Abel 扩域与 k^* 的所有闭子群之间同样的一一对应. 另一方面, 从 $\pi \in N(F_\phi/k)$, $KF_\phi = k_{ab}$ 容易得出 $N(F_\phi/k) = \langle \pi \rangle$. 从而 $N(k_x/k) = N(F_\phi/k) = \langle \pi \rangle$, 由此得到 $k_x = F_\phi$.

由于 $k^* = \langle \pi \rangle \times U$, 从而基本映射 $\rho_k: k^* \rightarrow \text{Gal}(k_{ab}/k)$ 由 $\rho_k(\pi)$ 和 $\rho_k(u) (u \in U)$ 所完全决定. 又由定理 4 知道

$$k_{ab} = k_{ur} k_x,$$

从而 $\rho_k(\pi)$ 由 $\rho_k(\pi)|_{k_{ur}}$ 和 $\rho_k(\pi)|_{k_x}$ 所完全决定. 但是由 § 6.2, 定理 5 和上面的定理 4 知道

$\rho_k(\pi)|_{k_{ur}} = k_{ur}/k$ 的 Frobenius 自同构, $\rho_k(\pi)|_{k_x} = 1$. 同样地, $\rho_k(u) (u \in U)$ 也由 $\rho_k(u)|_{k_{ur}}$ 和 $\rho_k(u)|_{k_x}$ 所完全决定, 而

$$\rho_k(u)|_{k_{ur}} = \sigma_k(u^{-1})|_{k_{ur}} = 1.$$

另一方面, $\rho_k(u)$ 在 $k_x = k(E_f)$ 上的作用, 即 $\rho_k(u)$ 在 E_f 上的作用按照定理 2 是

$$\rho_k(u)(\alpha) = [u^{-1}]f(\alpha), \alpha \in E_f.$$

换句话说, 如果知道了幂级数 $[u]f(X)$, $u \in U$, 则通过定理 2 和定理 4 可以将 k 的基本映射的意思具体地写出来. 下一章我们对于 $k = \mathbb{Q}$ 的情形作更详细的说明.

第八章 局部分圆域

局部分圆域是局部域中最简单也是最典型的例子。本章首先用前章的结果证明局部分圆域的基本性质，然后给出范剩余符号的一般定义，特别地对于局部分圆域证明 Artin-Hasse 公式。关于局部分圆域还有其他一些有趣味的结果，但是我们在这里对于局部分圆域这一特别情形作具体考查，其着眼点主要还是为了对于一般理论有更深入的理解。

§ 8.1 局部分圆域

一般地，在任意域 F 上添加所有 n 次单位根而得到的域叫作 F 上的 n -分圆域。熟知这是 F 的有限 Abel 扩域。以下对于任意素数 p 和自然数 n 考查 p -adic 数域 \mathbb{Q}_p 上的 n -分圆域。这种域通常叫作局部分圆域。由于 \mathbb{Q}_p 是局部域，从而局部分圆域是局部域的有限 Abe. 扩域的例子。今后我们固定 \mathbb{Q}_p 的一个代数闭包 $\bar{\mathbb{Q}}$ ，对于任意 $n \geq 1$ ，以 W_n 表示包含在 $\bar{\mathbb{Q}}$ 中的 n 次单位根全体：

$$W_n = \{\zeta \in \bar{\mathbb{Q}} \mid \zeta^n = 1\}.$$

由于 $\bar{\mathbb{Q}}$ 是特征为零的代数封闭域，从而 W_n 是 n 阶循环乘法群。以下用

$$C_n = \mathbb{Q}_p(W_n)$$

表示(包含在 $\bar{\mathbb{Q}}$ 中的) \mathbb{Q}_p 的 n -分圆域。

前章叙述的形式群一般理论中取

$$k = \mathbb{Q}_p, \pi = p.$$

\mathbb{Q}_p 的剩余类域为 $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ ，共有 p 个元素，从而 $q = p$ 。因此

$f(X) = (X+1)^p - 1 = X^p + pX^{p-1} + \cdots + pX$
 属于 § 7.2 中的 $\mathcal{F}_p(-\mathcal{F}_p)$. 令

$$F(X, Y) = (X+1)(Y+1) - 1,$$

则直接可得出

$$f(F(X, Y)) = F(f(X), f(Y)),$$

从而由 § 7.2 中的定义可知 $F = F_f$, 即

$$F_f(X, Y) = (X+1)(Y+1) - 1 = X + Y + XY.$$

又对于任意的 $a \in \mathbb{Z}_p$, 令

$$\phi_a(X) = (X+1)^a - 1 = \sum_{m=1}^{\infty} \binom{a}{m} X^m,$$

$$\binom{a}{m} = \frac{a(a-1)\cdots(a-m+1)}{m!},$$

则

$$f \circ \phi_a = \phi_a \circ f, \quad \phi_a(X) \equiv aX \pmod{\deg 2},$$

再由定义 (§ 7.2, 引理 3) 可知 $\phi_a(X) = [a]_f$, 即得到

$$[a]_f(X) = (X+1)^a - 1 = \sum_{m=1}^{\infty} \binom{a}{m} X^m, \quad a \in \mathbb{Z}_p.$$

由 $f = [\pi]_f = [p]_f$ 得出

$$f^{(n)}(X) = [p^n]_f(X) = (X+1)^{p^n} - 1.$$

与 § 7.3 的 $E_f^n, g(X) = X^p + \pi X$ 的情形一样, 令

$$E_f^n = \{\alpha \in \mathbb{Q} \mid f^{(n)}(\alpha) = 0\} = \{\alpha \in \mathbb{Q} \mid (\alpha+1)^{p^n} = 1\} = \{\zeta - 1 \mid \zeta \in W_{p^n}\}.$$

从而根据 § 7.3 的一般定义, 在这种情形下, k 的有限 Abel 扩域 $k_n^n = k(E_f^n)$ 为

$$k_n^n = \mathbb{Q}_p(E_f^n) = \mathbb{Q}_p(W_{p^n}) = C_{p^n}.$$

从而局部分圆域 C_{p^n} 即是 § 7.3 中 k_n^n 的特殊情形. \mathbb{Q}_p 的单位群 $U = U(\mathbb{Q}_p)$ 的子群 $U_i, i \geq 0$ 定义为

$$U_0 = U, \quad U_i = 1 + p^i \mathbb{Z}_p, \quad i \geq 1,$$

从而由 § 7.3, 定理 1 得到如下结果:

定理 1 局部分圆域 $C_{p^n} = \mathbb{Q}_p(W_{p^n}), n \geq 1$ 是 \mathbb{Q}_p 的有

根完全分歧 Abel 扩域, 并且

$$[C_{p^n}:Q_p] = (p-1)p^{n-1},$$

$$N(C_{p^n}/Q_p) = \langle p \rangle \times U_n.$$

从而 Q_p 的基本映射 $\rho: Q_p^\times \rightarrow \text{Gal}((Q_p)_{ab}/Q_p)$ 诱导出同构

$$Q_p^\times/N(C_{p^n}/Q_p) = U/U_n \xrightarrow{\sim} \text{Gal}(C_{p^n}/Q_p).$$

以上是从 § 7.3 的定理 1 直接推导出上述定理, 但是也不难直接证明, 即不依赖于形式群理论证明出来. 其方法说明如下: 由 § 4.1 所述, 设 \bar{Q} 是 Q_p 的代数闭包 Q 的完备化, Q_p 的正规赋值即 p -adic 赋值 v_p 到 \bar{Q} 有唯一的扩充 $\bar{\mu}$. 对于 \bar{Q} 中元素 ξ 可以定义 p -adic 指数函数和 p -adic 对数函数

$$\exp(\xi) = \sum_{n=0}^{\infty} \frac{1}{n!} \xi^n,$$

$$\log(1+\xi) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} \xi^n,$$

熟知右边幂级数分别当 $\bar{\mu}(\xi) > \frac{1}{p-1}$ 和 $\bar{\mu}(\xi) > 0$ 时在 \bar{Q} 中收敛, 并且满足

$$\exp(\xi_1 + \xi_2) = \exp(\xi_1)\exp(\xi_2),$$

$$\log((1+\xi_1)(1+\xi_2)) = \log(1+\xi_1) + \log(1+\xi_2),$$

并且在 $\bar{\mu}(\xi) > \frac{1}{p-1}$ 的时候,

$$\bar{\mu}(\exp(\xi) - 1) = \bar{\mu}(\xi), \quad \log(\exp(\xi)) = \xi,$$

$$\bar{\mu}(\log(1+\xi)) = \bar{\mu}(\xi), \quad \exp(\log(1+\xi)) = 1+\xi.$$

进而, 如果 ξ 是 Q_p 的有限扩域 k 中的元素, 由于 k 是完备域, 从而 $\exp(\xi)$ 和 $\log(1+\xi)$ 也属于 k . 特别对于 Q_p , $p > 2$, $\frac{1}{p-1} < 1$, 便得到加法群 pZ_p 和乘法群 $U_1 = 1 + pZ_p$ 之间彼此互逆的拓扑同构

$$\exp: pZ_p \xrightarrow{\sim} 1 + pZ_p, \quad \log: 1 + pZ_p \xrightarrow{\sim} pZ_p.$$

这一同构给出

$$U_1^{p^i} = U_{i+1} \cong p^{i+1} \mathbb{Z}_p, \quad i \geq 0.$$

当 $p = 2$ 时, $\frac{1}{p-1} = 1$, 从而

$$\exp: 4\mathbb{Z}_2 \xrightarrow{\sim} 1 + 4\mathbb{Z}_2, \quad \log: 1 + 4\mathbb{Z}_2 \xrightarrow{\sim} 4\mathbb{Z}_2,$$

$$U_i^2 = U_{i+2} \cong 2^{i+2} \mathbb{Z}_2, \quad i \geq 0.$$

取 ζ 为 \mathbb{Q} 中的 p^n 次本原单位根, $n \geq 1$, 又令 $\alpha = \zeta - 1$, 则

$$C_{p^n} = \mathbb{Q}_p(\zeta) = \mathbb{Q}_p(\alpha),$$

而 α 是 $\mathbb{Z}_p[X]$ 中 Eisenstein 多项式

$$\begin{aligned} h^{(n)}(X) &= ((X+1)^{p^n} - 1)/((X+1)^{p^{n-1}} - 1) \\ &= X^{(p-1)p^{n-1}} + \cdots + p \end{aligned}$$

的根, 从而得到

$$[C_{p^n} : \mathbb{Q}_p] = (p-1)p^{n-1}, \quad p = N_{C_{p^n}/\mathbb{Q}_p}(-\alpha),$$

从而 C_{p^n} 是 \mathbb{Q}_p 的完全分歧 Abel 扩张而 $\alpha = \zeta - 1$ 是 C_{p^n} 的素元. 并且由上述可知

$$N(C_{p^n}/\mathbb{Q}_p) = \langle p \rangle \times NU(C_{p^n}/\mathbb{Q}_p),$$

$$\mathbb{Q}_p^\times / N(C_{p^n}/\mathbb{Q}_p) = U / NU(C_{p^n}/\mathbb{Q}_p),$$

从而由对于 C_{p^n}/\mathbb{Q}_p 的基本等式得到

$$[U : NU(C_{p^n}/\mathbb{Q}_p)] = [C_{p^n} : \mathbb{Q}_p] = (p-1)p^{n-1}.$$

由 § 3.1, 定理 3 得到

$$U = V \times U_1, \quad V = W_{p-1}.$$

如果 $p > 2$, 则由上述可知 $U_1 \cong p\mathbb{Z}_p$, 从而 $NU(C_{p^n}/\mathbb{Q}_p)$ 是 U 的开子群, 于是由 $[U : NU(C_{p^n}/\mathbb{Q}_p)] = (p-1)p^{n-1}$ 立刻得到

$$NU(C_{p^n}/\mathbb{Q}_p) = U_1.$$

当 $p = 2$ 时,

$$V = 1, \quad U = U_1 = \langle -1 \rangle \times U_2, \quad C_2 = \mathbb{Q}_2(-1) = \mathbb{Q}_2,$$

$$C_4 = \mathbb{Q}_2(\sqrt{-1}),$$

显然有 $NU(C_4/\mathbb{Q}_2) = U_1$, 而对于 C_4 有 $U_1^2 = U_3$, 由于

$$5 \quad N_{C_4/\mathbb{Q}_2}(1 + 2\sqrt{-1}) \in NU(C_4/\mathbb{Q}_2),$$

从而 $NU(C_4/\mathbb{Q}_2) = U_1$. 当 $n \geq 2$ 时

$$\backslash NU(C_2^n/Q_2) \subseteq NU(C_4/Q_2) = U_2,$$

利用 $U_2 \cong 4\mathbb{Z}_2$, 可以与上面同样地得到 $NU(C_{2^n}/Q_2) = U_n$. 这就证明了定理 1.

如前所述, 对于 $k = Q_p$, $\pi = p$ 有 $k_n^\pi = Q_p(W_{p^n}) = C_{p^n}$, 如果令 W_{p^∞} 是所有 $W_{p^n} (n \geq 1)$ 之并, 则在这种情形下 § 7.3 中的 k_n 即为 $Q_p(W_{p^\infty})$:

$$k_n = Q_p(W_{p^\infty}).$$

W_{p^∞} 显然是由 Ω 中全部 $p^n (n \geq 1)$ 次单位根构成的. 如果以 W_∞ 表示 Ω 中全部单位根, V_∞ 表示阶与 p 互素的单位根全体, 则

$$W_\infty = V_\infty \times W_{p^\infty}, \quad Q_p(W_\infty) = Q_p(V_\infty)Q_p(W_{p^\infty}).$$

由 § 4.2 知道 $Q_p(V_\infty)$ 为局部域 Q_p 的极大不分歧扩域:

$$Q_p(V_\infty) = (Q_p)_{nr}.$$

此外, 如果 $n|m$, 则 $W_n \subseteq W_m$, $C_n \subseteq C_m$, 而 $Q_p(W_\infty)$ 是所有 $C_n = Q_p(W_n)$, $n \geq 1$ 之并集合. 从而由定理 4 中等式

$$k_{ab} = k_{ar}k_n$$

得到如下定理:

定理 2 p -adic 域 Q_p 的极大 Abel 扩域 $(Q_p)_{ab}$ 等于所有局部分圆域 $C_n = Q_p(W_n)$ ($n \geq 1$) 之并 $Q_p(W_\infty)$:

$$(Q_p)_{ab} = Q_p(W_\infty).$$

从而 Q_p 的任意有限 Abel 扩域 k 均是某个局部分圆域 C_n 的子域, 即存在适当的自然数 n , 使得 $Q_p \subseteq k \subseteq C_n$.

现在设 n 是与 p 互素的自然数, 由于

$$W_n \subseteq V_\infty, \quad C_n \subseteq Q_p(V_\infty),$$

从而 C_n/Q_p 是不分歧扩张. 它的次数 $[C_n:Q_p]$ 等于有限环 $\mathbb{Z}/n\mathbb{Z}$ 的乘法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ 中 $p \bmod n$ 的阶数. 证明可作为练习留给读者 (参见下节引理 2). 对于任意自然数 n , $n = n'p^a$, $(n', p) = 1$, $a \geq 0$. 显然 $C_n = C_{n'} \cdot C_{p^a}$, 由上述可知 $C_{n'}/Q_p$ 不分歧, 又由定理 1 可知 C_{p^a}/Q_p 完全分歧, 从而 $C_{n'} \cap C_{p^a} = Q_p$. 特别地,

$$[C_n:Q_p] = [C_{n'}:Q_p][C_{p^a}:Q_p].$$

于是由上面的注记和定理 1 即可计算次数 $[C_n:Q_p]$.

注记 如果 p 局部域 k 的特征为 p , 则 k 中单位根的阶必与 p 互素, 从而与上面所述同样的理由, 可知 k 的分圆域均是不分歧扩域. 反过来也成立. 但是如果 k 的特征为 0, 由 § 3.1, 定理 1 可知 k 为 Q_p 的有限扩域, 而 k 的 n -分圆域是合成域

$$kC_n = k(W_n).$$

这就是为什么我们在局部域的分圆域中, 特别地考查

$$C_n = Q_p(W_n).$$

现在设 X 是加法 Abel 群, 并且每个元素的阶均是素数 p 的幂. 如果 $a \in \mathbb{Z}_p, x \in X$, 当自然数 n 对于 p -adic 拓扑距离 a 很近的时候, nx 定义出 X 中同一元素, 我们由此定义 $ax = nx$, 从而 X 为 \mathbb{Z}_p 模. 如果 X 赋以离散拓扑, 则 $(a, x) \mapsto ax$ 是从 $\mathbb{Z}_p \times X$ 到 X 的连续映射. 将此用于乘法群 W_{p^m} , 则 \mathbb{Z}_p 作用于 W_{p^m} 上, 即对于任意 $a \in \mathbb{Z}_p, \zeta \in W_{p^m}$ 定义出 W_{p^m} 中元素 ζ^a . 另一方面, 令 $\zeta \in W_{p^m}$, 从而 $\alpha = \zeta - 1 \in E_f^m \subseteq m$, 令

$$[a]_f(\alpha) = \sum_{n=1}^{\infty} \binom{a}{n} \alpha^n,$$

则右边级数在 C_{p^m} 内收敛. 如果 a 是自然数, 则该级数的值显然为 $(\alpha + 1)^a - 1 = \zeta^a - 1$, 然后从对于 a 的连续性可知这对任意 $a \in \mathbb{Z}_p$ 均成立. 换句话说, 对于如上所述关于 ζ^a 的一般定义, 则对于每个 $a \in \mathbb{Z}_p, \zeta \in W_{p^m}, \alpha = \zeta - 1 \in E_f^m$, 均有

$$[a]_f(\alpha) = \zeta^a - 1.$$

定理 3 设

$$\rho: Q_p^\times \rightarrow \text{Gal}((Q_p)_{ab}/Q_p)$$

是局部域 Q_p 的基本映射, 则对于 Q_p 的单位群 $U = U(Q_p)$ 中每个元素 u 和 W_{p^m} 中每个元素 ζ , 均有

$$\rho(u)(\zeta) = \zeta^{u^{-1}}.$$

证明 令 $\sigma = \rho(u), \zeta \in W_{p^m}$. 由 § 7.3, 定理 2 可知对于 $\alpha = \zeta - 1 \in E_f^m$ 有

$$\sigma(\alpha) = [u^{-1}]_f(\alpha) = \zeta^{u^{-1}} - 1.$$

然后由 $\sigma(\alpha) = \sigma(\zeta) - 1$ 即得定理的等式.

根据这个定理, 当 $x \in \mathbf{Q}_p^\times$ 时, 我们可以将 $\rho(x)$ 在

$$(\mathbf{Q}_p)_{ab} = \mathbf{Q}_p(W_\infty)$$

上的作用, 即 $\rho(x)$ 在 W_∞ 上的作用具体地表达出来. 现在说明如下(参见 § 7.3 末尾的一般注记). W_∞ 中每个元素均可写成

$$\omega = \eta\zeta, \quad \eta \in V_\infty, \quad \zeta \in W_{p^\infty}.$$

设 k 是任意的局部域, 则对于 $u \in U$ 我们有

$$\rho_k(u) = \delta_k(u^{-1}), \quad \rho_k(u)|_{k_{ur}} = 1, \quad k_{ur} = k(V_\infty).$$

在现在的情况下, $\rho(u)(\eta) = \eta$, 从而由定理 3 得到

$$\rho(u)(\omega) = \eta\zeta^{u^{-1}}, \quad u \in U.$$

另一方面, 令 $\phi = \rho(p)$, 则由 § 7.3, 定理 4 可知

$$\mathbf{Q}_p(W_{p^\infty}) = k_\pi = F_\phi,$$

从而 $\rho(p)(\zeta) = \zeta$. 此外, ϕ 在 $(\mathbf{Q}_p)_{ur} = \mathbf{Q}_p(V_\infty)$ 上与 $(\mathbf{Q}_p)_{ur}/\mathbf{Q}_p$ 的 Frobenius 自同构一致, 从而由 § 4.2 可知

$$\phi(\eta) = \varphi(\eta) = \eta^p.$$

于是

$$\rho(p)(\omega) = \eta^p\zeta.$$

因此对于一般的 $x = p^m u$, $m \in \mathbf{Z}$, $u \in U$, 则

$$\rho(x)(\omega) = \eta^{p^m}\zeta^{u^{-1}}, \quad \omega = \eta\zeta \in W_\infty,$$

这就具体地决定出 $\rho(x)$ 在 W_∞ 上的作用.

注记 定理 3 最初是利用(整体)类域论的结果证明的. 后来 Dwork 给了一个只依赖局部域的证明, 从那里可以看到此处介绍的采用形式群证明的雏型. 但是所有这些方法都不能对定理 2 给出象定理 1 那样简单的证明.

对于有理数域 \mathbf{Q} 上的极大 Abel 扩域 \mathbf{Q}_{ab} , 我们有熟知的 Kronecker 定理, 即 \mathbf{Q}_{ab} 是由 \mathbf{Q} 添加全部单位根而得到的. 换句话说, 对于有理数域 \mathbf{Q} 也有类似于定理 2 的结果. 作为定理 2 的应用, 现在我们来证明 Kronecker 定理. 但是需要假定我们知道关于代数数域的某些事实.

设 F 是 \mathbf{Q} 的任意有限 Abel 扩域, 以 p_1, \dots, p_r 表示在 F

中分歧的全部素数. 由于 FQ_{p_i} ($1 \leq i \leq s$) 是 Q_{p_i} 的有限 Abel 扩域, 根据定理 2 可知存在自然数 n_i , 使得 FQ_{p_i} 包含在 Q_{p_i} 的 n_i -分圆域之中. 又设

$$n = \prod_{i=1}^s n_i = \prod_{j=1}^t q_j^{\alpha_j}, \quad \alpha_j \geq 1.$$

其中 q_1, \dots, q_t 是不同的素数. 令 K 为 Q 的 n -分圆域, $L = FK$, 则 L 也是 Q 的有限 Abel 扩域. 下面对于每个素数 p 计算 p 在 L 中的分歧指数, 即局部扩张 LQ_p/Q_p 的分歧指数 e_p .

i) $p = p_i$ ($1 \leq i \leq s$) 的情形. 由 n 和 n_i 的定义可知

$$FQ_{p_i} \subseteq KQ_{p_i},$$

从而 $LQ_{p_i} = KQ_{p_i}$, 于是 e_{p_i} 等于 p_i 在 K 中的分歧指数. 如果 p_i 在 F 中分歧, 则 $e_{p_i} > 1$. 另一方面, K 是 n -分圆域, 则当 $e_{p_i} > 1$ 时 $p_i | n$, 即 p_i 为 q_1, \dots, q_t 当中的某一个. 如果 $p_i = q_j$, 则由 n -分圆域 K 的性质可知 $e_{p_i} = e_{q_j} = \varphi(q_j^{\alpha_j})$. 其中 φ 为 Euler 函数.

ii) $p \neq p_1, \dots, p_s$, 但是 $p = q_j$ ($1 \leq j \leq t$) 的情形. 由于 p 在 F 中不分歧, 从而 $e_p = e_{q_j}$ 等于 q_j 在 K 中的分歧指数, 与上面一样地 $e_p = e_{q_j} = \varphi(q_j^{\alpha_j})$.

iii) $p \neq q_1, \dots, q_t$ 的情形. 这时从 i) 可知也有 $p \neq p_1, \dots, p_s$. 从而 p 在 $L = FK$ 中不分歧, 于是 $e_p = 1$.

设 L_j 是 q_j 在 L 中的惯性域, 则由 i) 和 ii) 可知

$$[L:L_j] = e_{q_j} = \varphi(q_j^{\alpha_j}) \quad (1 \leq j \leq t).$$

又由 iii) 可知每个素数在 $\bigcap_{j=1}^t L_j$ 中均不分歧, 于是由 Minkowski 定理¹⁾ 可知

$$\bigcap_{j=1}^t L_j = Q.$$

从而

1) Minkowski 定理是说: 有理数域 Q 的最大不分歧扩域是它自身. ——译者注

$$\begin{aligned}[L:Q] &\leq \prod_{i=1}^t [L:L_i] \\ &= \prod_{i=1}^t \varphi(q_i^a) = \varphi(n) = [K:Q].\end{aligned}$$

但是 $Q \subseteq K \subseteq L$, 于是得到

$$K = L, F \subseteq K.$$

由于 F 是 Q 的任意有限 Abel 扩域而 K 是分圆域, 这就证明了 Kronecker 定理.

§ 8.2 范剩余符号

设 F 是任意域, A 是任意乘法 Abel 群, 则满足如下条件 i) 和 ii) 的映射

$$(\cdot, \cdot): F^\times \times F^\times \rightarrow A$$

叫作是 F 上取值于 A 的符号 (symbol)¹⁾, 其中

i) 对于 F 中任意元素 x, y, x', y' ,

$$(x, yy') = (x, y)(x, y'), \quad (xx', y) = (x, y)(x', y).$$

ii) 如果 $x \neq 0, 1$, 则

$$(x, 1-x) = 1.$$

符号 (x, y) 有如下的简单性质. 首先从 i) 可知

$$(1, x) = (x, 1) = 1, \quad (x, y^{-1}) = (x^{-1}, y) = (x, y)^{-1}.$$

从而当 $x \neq 0, 1$ 时, ii) 和 $(1-x, x) = 1$ 是一回事.

引理 1 i) $(x, -x) = 1, (x, y) \cdot (y, x) = 1.$

ii) $z = x + y \neq 0$, 则 $(x, y) = (x, z)(z, y)(-1, z).$

证明 i) 可设 $x \neq 1$. 由于 $(x, 1-x) = 1$, 从而

$$(x, 1-x)^{-1} = (x^{-1}, 1-x^{-1}) = 1.$$

于是

1) 关于符号的一般理论可参见 Minor [10].

$$(x, -x) = \left(x, \frac{1-x}{1-x^{-1}}\right)$$

$$(x, 1-x)(x, 1-x^{-1})^{-1} = 1,$$

从而 $(x, y) = (x, y)(x, -x) = (x, -x)$. 同样地

$$(y, x) = (y, -yx).$$

从而 $(x, y)(y, x) = (xy, -xy) = 1$.

ii) 由于 $(x/z, y/z) = (x/z, 1-x/z) = 1$, 从而

$$(x, y)(z, y)^{-1}(x, z)^{-1}(z, z) = 1.$$

再由

$$(z, z) = (z, -1)(z, -z) = (z, -1) = (-1, z)^{-1}$$

即证.

以下研究 F 是局部域的情形. 首先证明如下的引理.

引理 2 任意局部域 k 中单位根全体 W 是有限循环群. 如果 k 是 p 局部域, q 是 k 的剩余类域的元素个数, 则 W 的阶数可以写成

$$w = (q-1)p^a, \quad a \geq 0.$$

特别又若 k 的特征为 p , 则 $w = q-1$.

证明 设 U 是 p 局部域 k 的单位群. k 的正规赋值 v 显然给出同构 $k^\times/U \cong \mathbf{Z}$. 从而 $W \subseteq U$. 由 § 3.1, 定理 3 可知

$$U = V \times U_1.$$

而 V 是 U 的 $q-1$ 阶子群. 从而 $V \subseteq W$. 又由 § 3 中所述, 知道 U_1 是射影 p 群, 从而对于每个与 p 互素的 m , $u \mapsto u^m$ 给出 U_1 的自同构. 从而 V 即是 k 中阶数与 p 互素的单位根全体. 如果 k 的特征是 p , 则 k 中单位根的阶数均与 p 互素, 从而由上述即知

$$W = V, \quad w = q-1.$$

如果 k 的特征是 0 并且 k 包含 p^n 次本原单位根, 则

$$Q_p \subseteq C_{p^n} = Q_p(W_{p^n}) \subseteq k.$$

由定理 1 我们有

$$(p-1)p^{n-1} = [C_{p^n}:Q_p] \leq [k:Q_p],$$

从而 n 是有界的. 再加上关于 V 的结果, 即知 W 是有限群, 并且

$w = (q - 1)p^a, a \geq 0$. 最后, k^\times 的有限子群 W 必然是循环群.

以下设局部域 k 包含 n 次本原单位根, 以 W_n 表示 k 中的 n 次单位根全体. 由引理 2 可知

$$n \mid w, W_n \subseteq W.$$

假设 y 是 k^\times 中任意元素, \bar{Q} 为 k 的代数闭包, 以 $\sqrt[n]{y}$ 表示 y 在 \bar{Q} 中任意一个 n 次根, 由上面假定可知 $k(\sqrt[n]{y})/k$ 是 Abel 扩张. 从而

$$k \subseteq k(\sqrt[n]{y}) \subseteq k_{ab}.$$

设 $\rho_k: k^\times \rightarrow \text{Gal}(k_{ab}/k)$ 为 k 的基本映射, 对于 k^\times 中元素 x , 令 $\sigma = \rho_k(x)$, 并且定义

$$(\sqrt[n]{y})^{\sigma^{-1}} = \sigma(\sqrt[n]{y})/\sqrt[n]{y}.$$

由于 $y^{\sigma^{-1}} = 1$, 因此 $(\sqrt[n]{y})^{\sigma^{-1}} \in W_n$. 另一方面, y 的两个 n 次根的商也属于 W_n , 从而是 σ 不变的, 因此元素 $(\sqrt[n]{y})^{\sigma^{-1}}$ 只依赖于 x 和 y . 从而定义

$$(x, y)_n = (\sqrt[n]{y})^{\sigma^{-1}}, \sigma = \rho_k(x).$$

即得到映射

$$(\cdot, \cdot)_n: k^\times \times k^\times \rightarrow W_n.$$

引理 3 上面定义的 $(x, y)_n$ 是取值于 W_n 的符号.

证明 由于 $\sqrt[n]{yy'} = \sqrt[n]{y} \sqrt[n]{y'}$, 从而

$$(x, yy') = (x, y)(x, y').$$

令 $\sigma = \rho_k(x), \sigma' = \rho_k(x')$, 从而 $\sigma\sigma' = \rho_k(xx')$, 由

$$(\sqrt[n]{y})^{\sigma'^{-1}} \in W$$

可知

$$\begin{aligned} (xx', y)_n &= (\sqrt[n]{y})^{\sigma\sigma'^{-1}} = (\sqrt[n]{y})^{\sigma^{-1}} ((\sqrt[n]{y})^{\sigma'^{-1}})^\sigma \\ &= (\sqrt[n]{y})^{\sigma^{-1}} (\sqrt[n]{y})^{\sigma'^{-1}} = (x, y)(x', y). \end{aligned}$$

其次, 设 $x \neq 0, 1, k' = k(\sqrt[n]{x}), d = [k':k]$, 则 $d \mid n$, 当 η 过 d 次单位根时, $\eta \sqrt[n]{x}$ 组成 $\sqrt[n]{x}$ 在 k 上的全部共轭元素. 令 $W_n = \langle \zeta \rangle$, 则

$$\begin{aligned}
1-x &= \prod_{i=1}^n (1 - \zeta^i \sqrt[n]{x}) = \prod_{i=1}^{n/d} \prod_{\eta} (1 - \eta \zeta^i \sqrt[n]{x}) \\
&= N_{k'/k} \left(\prod_{i=1}^{n/d} (1 - \zeta^i \sqrt[n]{x}) \right) \in N(k'/k).
\end{aligned}$$

于是由 § 6.2, 定理 5 可知 $\rho_k(1-x) \mid k' = 1$. 从而

$$(1-x, x)_n = 1.$$

我们将 $(x, y)_n$ 叫作局部域 k 上的 n 次范剩余符号.

注记 k 上的 n 次范剩余符号也可以定义成

$$(x, y)_n = (\sqrt[n]{x})^{\sigma-1}, \quad \sigma = \rho_k(y).$$

按照引理 1, 如此定义的 $(x, y)_n$ 是早先定义的 $(x, y)_n$ 的逆元素. 从而这两个定义之间没有什么本质的不同.

定理 4 设 $(x, y)_n$ 是局部域 k 上的 n 次范剩余符号, 则

- i) $(x, y)_n = 1 \iff x \in N(k(\sqrt[n]{y})/k)$
 $\iff y \in N(k(\sqrt[n]{x})/k),$
- ii) $(x, k^\times)_n = 1 \iff (k^\times, x)_n = 1 \iff x \in (k^\times)^n,$
- iii) $(x, y)_n$ 作为变量 x 和 y 的函数对于 p -adic 拓扑是连续的.

证明 i)

$$\begin{aligned}
(x, y)_n = 1 &\iff \rho_k(x) \mid k(\sqrt[n]{y}) = 1 \\
&\iff x \in N(k(\sqrt[n]{y})/k) \\
&\iff (y, x)_n = 1 \\
&\iff y \in N(k(\sqrt[n]{x})/k) \quad (\S 6.3, \text{定理 } 7).
\end{aligned}$$

ii) 显然 $x \in (k^\times)^n \Rightarrow (x, k^\times)_n = (k^\times, x)_n = 1$. 其次若

$$x \notin (k^\times)^n,$$

则 $k' = k(\sqrt[n]{x}) \not\cong k$, $\text{Gal}(k'/k) \neq 1$. 从而由

$$\rho_{k'/k}: k^\times/N(k'/k) \xrightarrow{\sim} \text{Gal}(k'/k)$$

可知存在 $y \in k^\times$ 满足 $\rho_k(y) \mid k' \neq 1$. 于是

$$(y, x)_n = (\sqrt[n]{x})^{\sigma-1} \neq 1, \quad \sigma = \rho_k(y).$$

从而 $(k^\times, x)_n \neq 1, (x, k^\times)_n \neq 1$.

iii) 设 k 是 p 局部域并且特征为 p , 则由 $n|w$ 和引理 2 可知 n 与 p 互素. 于是由 § 3.1, 引理 2 可知 k 的特征无论是 0 还是 p , $k^{\times n}$ 均是 k^{\times} 的子群. 从而由 ii) 便知 $(x, y)_n$ 是对于 x 和 y 的连续函数.

从上述定理可知, 局部域 k 上的范剩余符号 $(x, y)_n$ 自然定义出斜对称非退化双线性型

$$k^{\times}/k^{\times n} \times k^{\times}/k^{\times n} \rightarrow W_n.$$

如果域 F 包含 n 次本原单位根, 则对于 F 上指数 (exponent) 为 n 的 Abel 扩域可以应用 Kummer 扩张理论. 特别若 F 为局部域, 则作为 Abel 扩域它又具有局部类域论. 所以对于同一个扩域可以同时应用 Kummer 扩张理论和局部类域论. 这两个理论相互交错的地方便产生出范剩余符号 $(x, y)_n$ 和上面的双线性型. 此外可以证明对于 $n = w$ 的情形, $(x, y)_n$ 是局部域 k 的最一般的连续符号 (C. Moore 定理, Milnor [10], 参见附录).

现在介绍两个公式, 它们反映出 $(x, y)_n$ 和局部域 k 之间的依赖关系. 首先令 σ 是 § 6.2 一开始所述的从局部域 (k, ν) 到 (k', ν') 的同构映射. σ 将 k 中的 n 次单位根全体 W_n 映到 k' 中 n 次单位根集合 W'_n 之上, 我们可以定义 k' 上的 n 次范剩余符号

$$(\cdot, \cdot)'_n: k'^{\times} \times k'^{\times} \rightarrow W'_n,$$

并且 $(x, y)_n^{\sigma} = (x^{\sigma}, y^{\sigma})'_n$, $x, y \in k^{\times}$. 这一事实由范剩余符号的定义和 § 6.2, 定理 2 (即 $\rho_{k'}(x^{\sigma}) = \sigma \rho_k(x) \sigma^{-1} x \in k^{\times}$) 即可证明. 如果 k' 是 k 的任意有限扩域, 则 $W_n \subseteq k'^{\times}$. 由此可以定义

$$(\cdot, \cdot)_n: k'^{\times} \times k'^{\times} \rightarrow W_n,$$

并且满足

$$(x', y)'_n = (N_{k'/k}(x'), y)_n, \quad x' \in k'^{\times}, y \in k^{\times}.$$

这一事实类似地可由 § 6.2, 定理 3 (即 $\rho_{k'}(x')|_{k_{ab}} = \rho_k(N_{k'/k}(x'))$) 得到证明.

k 和 n 如上所述. 如果 $m|n$, $m \geq 1$, 则 $W_m \subseteq W_n \subseteq k^{\times}$, 因

此在定义了 k 上的 m 次范剩余符号 $(x, y)_m$ 之后, 显然有

$$\sqrt[m]{y} = (\sqrt[n]{y})^{n/m},$$

从而得到

$$(x, y)_m = (x, y)_{n/m}^{n/m}.$$

一般地, 如果假定

$$n = n_1 n_2, n_1, n_2 \geq 1, (n_1, n_2) = 1,$$

则

$$an_1 + bn_2 = 1, a, b \in \mathbb{Z},$$

从而由上面公式给出

$$(x, y)_n = (x, y)_{n_1}^{an_1 + bn_2} = (x, y)_{n_1}^a (x, y)_{n_2}^b, x, y \in k^\times.$$

于是我们将计算 $(x, y)_n$ 的值归结为计算 $(x, y)_{n_1}$ 和 $(x, y)_{n_2}$. 如果以 W 表示 p 局部域 k 中单位根全体, 由引理 2 可知 W 的阶数是

$$w = (q - 1)p^a, a \geq 0.$$

于是 k 上的所有的范剩余符号均可由 $(x, y)_{q-1}$ 和 $(x, y)_{p^a}$ 所完全决定.

我们先考查 $(x, y)_{q-1}$. 象引理 2 的证明中所讲的那样, 如果令 $U = V \times U_1$, 而 \mathfrak{f} 是 k 的剩余类域, 则由 § 3.1, 引理 1 的系可知 $V \cong \mathfrak{f}^\times$. 从而 V 中元素 $(x, y)_{q-1}$ 由它在 $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ 中的剩余类所完全确定. 于是 $(x, y)_{q-1}$ 的值可由下面定理给出, 即:

定理 5 设 ν 是局部域 k 的正规赋值, q 为 k 的剩余类域

$$\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$$

的元素个数, 则对于 k 中任意元素 x, y 我们有

$$(x, y)_{q-1} \equiv (-1)^{\nu(x)\nu(y)} x^{-\nu(y)} y^{\nu(x)} \pmod{\mathfrak{p}}.$$

证明 上面同余式两边对于 x 和 y 均是积性的. 又由于 k^\times 是由 k 中素元集合 $\{\pi\}$ 所生成的, 因此只需对 k 中素元 $x = \pi$ 和 $y = -u\pi (u \in U)$ 证明这一同余式即可. 这时由引理 1 可知左边为

$$(\pi, -u\pi)_{q-1} = (\pi, u)_{q-1} (\pi, -\pi)_{q-1} = (\pi, u)_{q-1}.$$

而右边显然是 u . 根据 § 3.1 知道 $U = V \times U_1$, $U_1^{q-1} = U_1$, 因

此若令 $u = vu_1^{q-1}$, $v \in V$, $u_1 \in U_1$, $u_1 \equiv 1 \pmod{p}$, 则

$$k' = k(\sqrt[q-1]{u}) = k(\sqrt[q-1]{v}) \subseteq k(V_\infty) = k_{ur}.$$

另一方面, $\rho_k(\pi)|_{k_{ur}}$ 等于 k_{ur}/k 的 Frobenius 自同构. 从而对于 $\eta \in V_\infty$ 我们有 $\eta^q = \eta^q$ (参见 § 4.2), 因此

$$(\pi, u)_{q-1} = (\sqrt[q-1]{u})^{q-1} = (\sqrt[q-1]{v})^{q-1} = v \equiv u \pmod{p}.$$

这就证明了定理.

注记 对于任意的 $x, y \in k^\times$, 由同余式定义

$$s(x, y) \equiv (-1)^{v(x)v(y)} x^{-v(y)} y^{v(x)} \pmod{p},$$

可以不用范剩余符号的性质直接证明出 $s(x, y)$ 是取值于 V 的 k 上的符号. (参照 Milnor [10], p. 98.)

现在考虑 $(x, y)_{p^a}$. 当 $a = 0$ 时显然恒有 $(x, y)_{p^a} = 1$. 以下假定 $a \geq 1$. 这时根据引理 2 可知 k 是特征为 0 的 p 局部域, 并且包含 p^a 次本原单位根 ζ , $a \geq 1$:

$$\mathbf{Q}_p \subseteq \mathbf{Q}_p(\zeta) \subseteq k.$$

对于这样的 k , 范剩余符号 $(x, y)_{p^a}$ 没有象上面定理那样简单的一般结果. 作为例子, 这里对一个非常特别的情形, 即 k 是 \mathbf{Q}_p 的 p -分圆域并且 $a = 1$ 的情形 ($k = \mathbf{C}_p = \mathbf{Q}_p(\zeta)$, $\zeta^p = 1$, $\zeta \neq 1$) 来考查 $(x, y)_p$.

先设 $p = 2$, 即 $k = \mathbf{C}_2 = \mathbf{Q}_2(-1) = \mathbf{Q}_2$, $\zeta = -1$. 根据上节所述, 对于这种情形:

$$\mathbf{Q}_2^\times = \langle 2 \rangle \times U = \langle 2 \rangle \times \langle -1 \rangle \times U_2,$$

$$U = U_1, U_2^2 = U_3.$$

对于 $U = U_1$ 中任意元素 u 令

$$\varepsilon(u) = \frac{u-1}{2}, \quad \eta(u) = \frac{u^2-1}{8},$$

则 $\varepsilon(u)$ 和 $\eta(u)$ 均属于 \mathbf{Z}_2 , 并且显然有

$$u \equiv 1 \pmod{4} \Rightarrow \varepsilon(u) \equiv 0 \pmod{2},$$

$$u \equiv -1 \pmod{4} \Rightarrow \varepsilon(u) \equiv 1 \pmod{2},$$

$$u \equiv \pm 1 \pmod{8} \Rightarrow \eta(u) \equiv 0 \pmod{2},$$

$$u \equiv \pm 3 \pmod{8} \Rightarrow \eta(u) \equiv 1 \pmod{2}.$$

从而

$$s(uv) = s(u) + s(v) \bmod 2,$$

$$\eta(uv) = \eta(u) + \eta(v) \bmod 2.$$

定理 6 设 u, v 为 $U = U(Q_2)$ 中任意元素, 则

$$(u, v)_2 = (-1)^{s(u)s(v)},$$

$$(u, 2)_2 = (2, u)_2 = (-1)^{\eta(u)}, \quad (2, 2)_2 = 1.$$

证明 由于 $(x, y)_2 = \pm 1$, 从而首先有

$$(y, x)_2 = (x, y)_2^{-1} = (x, y)_2.$$

由上述可知 $(-1)^{s(u)s(v)}$ 和 $(-1)^{\eta(u)}$ 对于 u 均是积性的函数, 并且只依赖于 $u \bmod 8$. 另一方面, $U_2 = U_2^2$, $U/U_2 = (\mathbf{Z}_2/8\mathbf{Z}_2)^\times$, 从而 $(u, v)_2$ 和 $(u, 2)_2$ 也只依赖于 $u \bmod 8$. 因此我们只需对于 $u = -1$ 和 $u = 5$ 证明上面公式即可.

先考虑 $u = -1$, $s(-1) = -1$, $\eta(-1) = 0$ 的情形. 从前节定理 1 可知

$$N(Q_2(\sqrt{-1})/Q_2) = N(C_4/Q_2) = \langle 2 \rangle \times U_2,$$

于是由定理 4, i) 即知 $(-1, 2)_2 = 1 = (-1)^{\eta(-1)}$. 并且

$$(-1, v)_2 = 1 \iff v \in U_2 \iff v \equiv 1 \bmod 4.$$

由于 $(-1, v)_2 = \pm 1$, 因此

$$(-1, v)_2 = (-1)^{s(v)} = (-1)^{s(-1)s(v)}.$$

再考虑 $u = 5$, $s(5) = 2$, $\eta(5) = 3$ 的情形. 设 α 是

$$X^2 + X - 1$$

的根, 即 $\alpha = \frac{-1 + \sqrt{5}}{2}$, 则 $Q_2(\sqrt{5}) = Q_2(\alpha)$. 由于 $X^2 + X - 1$ 在 Q_2 的剩余类域 $\mathbf{Z}/2\mathbf{Z}$ 上不可约, 从而 $Q_2(\alpha)/Q_2$ 是 2 次不分歧扩张. 于是由 § 3.3, 引理 4 可知

$$N(Q_2(\sqrt{5})/Q_2) = \langle 4 \rangle \times U.$$

从而 $2 \nmid N(Q_2(\sqrt{5})/Q_2)$. 再由定理 4, i) 即知

$$(5, 2)_2 = -1 = (-1)^{\eta(5)}, \quad (5, v)_2 = 1 = (-1)^{s(5)s(v)}.$$

最后由引理 1 可知

$$(2, 2)_2 = (-1, 2)_2(-2, 2)_2 = (-1, 2)_2 = 1.$$

这就证明了定理.

对于 $p > 2$ 的情形, 这时关于 $(x, y)_p$ 有优美的 Artin Hasse 公式. 为了对证明公式作准备, 我们在下节先介绍局部域上的微分和它所定义出的同态.

§ 8.3 局部域上的微分

设 k_0 为任意局部域, k 为 k_0 的有限完全分歧扩域. k_0 和 k 的正规赋值与剩余类域分别记成 $v_0, f_0 = \mathfrak{o}_0/\mathfrak{p}_0$ 和 $v, f = \mathfrak{o}/\mathfrak{p}$. 再固定 k 中一个素元 $\pi: \mathfrak{p} = (\pi)$. 又设

$$h(X) = x^d + c_1 x^{d-1} + \cdots + c_d$$

是以 π 为根的 $k_0[X]$ 中不可约多项式. 由 § 1.3 中的注记可知 $k = k_0(\pi)$. 于是

$$d = [k:k_0], \quad c_d = \pm N_{k/k_0}(\pi), \quad v_0(c_d) = 1,$$

即 c_d 是 k_0 的素元. 由 § 1.2, 引理 4 知 π 对于 \mathfrak{o}_0 是整元, 从而 $h(X) \in \mathfrak{o}_0[X]$. 特别由于 k/k_0 完全分歧, 根据 § 1.3 可知

$$\mathfrak{o} = \mathfrak{o}_0[[\pi]].$$

以 $\mathfrak{o}_0[[X]]$ 表示系数属于 \mathfrak{o}_0 的 X 之幂级数全体, 于是有满射的 \mathfrak{o}_0 模同态:

$$\begin{aligned} \mathfrak{o}_0[[X]] &\rightarrow \mathfrak{o}_0[[\pi]], \\ f(X) &\mapsto f(\pi). \end{aligned}$$

引理 4 上述同构的核是由 $h(X)$ 生成的主理想.

证明 由于 $h(\pi) = 0$, 从而 $h(X)$ 属于核中. 如果

$$f(X) = \sum_{n=0}^{\infty} a_n X^n \in \mathfrak{o}_0[[X]],$$

$$f(\pi) = \sum_{n=0}^{\infty} a_n \pi^n = 0,$$

则

$$a_0 = - \sum_{n=1}^{\infty} a_n \pi^n.$$

从而 $v(a_0) > 0$, 于是 $v_0(a_0) \geq 1$. 但是 $v_0(c_d) = 1$, 从而 $a_0 = b_0 c_d$, $b_0 \in \mathfrak{o}_0$. 于是 $f_1(X) = f(X) - b_0 h(X) \in \mathfrak{o}_0[[X]]$, 由 b_0 的定义和 $f(\pi) = h(\pi) = 0$ 可知

$$f_1(X) = \sum_{n=1}^{\infty} a'_n X^n, \quad f_1(\pi) = 0.$$

于是 $a'_1 = -\sum_{n=2}^{\infty} a''_n \pi^{n-1}$, 又有 $v_0(a'_1) \geq 1$, $a'_1 = b_1 c_d$, $b_1 \in \mathfrak{o}_0$, 令 $f_2(X) = f_1(X) - b_1 X h(X) = f(X) - (b_0 + b_1 X) h(X)$, 则

$$f_2(X) = \sum_{n=2}^{\infty} a''_n X^n \in \mathfrak{o}_0[[X]], \quad f_2(\pi) = 0.$$

依此类推地决定出 \mathfrak{o}_0 中元素 b_2, b_3, \dots , 显然有

$$f(X) = \left(\sum_{n=0}^{\infty} b_n X^n \right) h(X).$$

从而证明了引理.

上面不可约多项式 $h(X)$ 的导函数 $h'(X) = dh/dX$ 属于 $\mathfrak{o}_0[X]$, 从而 $h'(\pi) \in \mathfrak{o}$. 令 \mathfrak{d} 为由 $h'(\pi)$ 生成的 \mathfrak{o} 的主理想:

$$\mathfrak{d} = (h'(\pi)).$$

对于 k 中另一个素元 π_1 , 令 $h_1(X)$ 是 $\mathfrak{o}_0[X]$ 中不可约多项式并且以 π_1 为根, 则

$$\pi_1 = \omega(\pi), \quad \omega(X) = \sum_{n=1}^{\infty} \omega_n X^n, \quad v_0(\omega_1) = 0,$$

$$h_1(\omega(\pi)) = h_1(\pi_1) = 0.$$

由引理 4 可知

$$h_1(\omega(X)) = g(X)h(X), \quad g(X) \in \mathfrak{o}_0[[X]].$$

两边对 X 求微商然后令 $X = \pi$, 便得到

$$h'_1(\pi_1)\omega'(\pi) = g(\pi)h'(\pi),$$

其中 $\omega'(\pi) = \omega_1 + 2\omega_2\pi + \dots$, $v_0(\omega_1) = 0$, 从而

$$v(\omega'(\pi)) = 0.$$

即 $\omega'(\pi) \in U$, 由上面等式可知 $h'_1(\pi_1) \in \mathfrak{d} = (h'(\pi))$. 基于同样的理由则 $h'(\pi) \in (h'_1(\pi))$. 因此

$$\mathfrak{d} = (k'(\pi)) \cdot (k'(\pi_1)).$$

换句话说, 作为 \mathfrak{o} 中的理想, \mathfrak{d} 是由扩张 k/k_0 所决定的而与 k 中素元 π 的取法无关. 事实上, 如果 k/k_0 是可分扩张, 通常将上面的 \mathfrak{d} 叫作 k/k_0 的共轭差积而略去“理想”二字¹⁾. 注意若 k/k_0 是不可分扩张, 则 $k'(\pi) = 0$ 从而 $\mathfrak{d} = 0$.

对 \mathfrak{o} 中任意元素 α , 如果

$$\alpha = f(\pi) + g(\pi), \quad f(X), g(X) \in \mathfrak{o}_0[[X]],$$

则由引理 4 可知

$$f(X) + g(X) = u(X)h(X), \quad u(X) \in \mathfrak{o}_0[[X]].$$

两边对 X 微商然后令 $X = \pi$, 则

$$f'(\pi) + g'(\pi) = u(\pi)h'(\pi),$$

从而

$$f'(\pi) \equiv g'(\pi) \pmod{\mathfrak{d}}.$$

因此 $\mathfrak{o}/\mathfrak{d}$ 中 $f'(\pi)$ 所在的剩余类是由 α 所确定的, 定义映射

$$\begin{aligned} D_\pi: \mathfrak{o} &\rightarrow \mathfrak{o}/\mathfrak{d} \\ \alpha &\longmapsto f'(\pi) \pmod{\mathfrak{d}}, \end{aligned}$$

D_π 显然是 \mathfrak{o}_0 -模同态, 并且满足

$$\begin{aligned} D_\pi(\alpha\beta) &= \alpha D_\pi(\beta) + D_\pi(\alpha)\beta, \quad \alpha, \beta \in \mathfrak{o}, \\ D_\pi(\pi) &= 1 \pmod{\mathfrak{d}}. \end{aligned} \tag{1}$$

换句话说, D_π 是 \mathfrak{o} 上取值于 $\mathfrak{o}/\mathfrak{d}$ 的 \mathfrak{o}_0 -微分. 并且不难看出, D_π 是满足 $D(\pi) = 1$ 的唯一微分 D .

现在设 α 是 k 的单位群 U 中任意元素, 令

$$\delta_\pi(\alpha) = \frac{D_\pi(\alpha)}{\alpha} = \frac{f'(\pi)}{\alpha} \pmod{\mathfrak{d}}.$$

由于 $1/\alpha \in \mathfrak{o}$, 从而右边为 $\mathfrak{o}/\mathfrak{d}$ 中元素, 并且由 (1) 式可知

$$\delta_\pi(\alpha\beta) = \delta_\pi(\alpha) + \delta_\pi(\beta), \quad \alpha, \beta \in U.$$

换句话说,

$$\delta_\pi: U \rightarrow \mathfrak{o}/\mathfrak{d}$$

1) 关于共轭差积请参考 [1], 提到的 Artin [2] 和 Serre [11].

是乘法群 U 到加法群 $\mathfrak{o}/\mathfrak{d}$ 的同态. 由于 $k^\times = \langle \pi \rangle \times U$, 从而上面的 $\delta_\pi: U \rightarrow \mathfrak{o}/\mathfrak{d}$ 通过

$$\delta_\pi(\pi) = \frac{1}{\pi} \bmod \mathfrak{d}$$

唯一地扩充成同态

$$\delta_\pi: k^\times \rightarrow \mathfrak{o}^{-1}/\mathfrak{d}, \quad \pi^{-1} = \frac{1}{\pi} \mathfrak{o}.$$

现在说明对 \mathfrak{o} 中每个元素 $\alpha \neq 0$ 如何计算 $\delta_\pi(\alpha)$. 根据假设, $v(\alpha) = m \geq 0$, 从而 $\alpha = \pi^m \beta$, $\beta = g(\pi) \in U$, $g(X) \in \mathfrak{o}_0[[X]]$. 令 $f(X) = X^m g(X)$, 则

$$\alpha = f(\pi), \quad f(X) = \sum_{n=m}^{\infty} a_n X^n, \quad a_n \in \mathfrak{o}_0, \quad v(a_m) = 0. \quad (2)$$

反之, 如果 $f(X)$ 为如上所示的幂级数, 令

$$f(X) = X^m g(X), \quad g(X) \in \mathfrak{o}_0[[X]],$$

则 $\alpha = \pi^m \beta$, $\beta = g(\pi) \in U$. 将 $f(X) = X^m g(X)$ 微分然后令 $X = \pi$, 再用 α 去除即得到

$$\frac{f'(\pi)}{\alpha} = \frac{m}{\pi} + \frac{g'(\pi)}{\beta}.$$

由于 $f'(\pi)/\alpha \in \mathfrak{o}^{-1}$,

$$\delta_\pi(\pi) = \frac{1}{\pi} \bmod \mathfrak{d}, \quad \delta_\pi(\beta) = \frac{g'(\pi)}{\beta} \bmod \mathfrak{d},$$

从而得出

$$\delta_\pi(\alpha) = \frac{f'(\pi)}{\alpha} \bmod \mathfrak{d}.$$

换句话说, \mathfrak{o} 中每个元素 $\alpha \neq 0$, $v(\alpha) = m \geq 0$ 表示成(2)的形式的时候, $\delta_\pi(\alpha)$ 具有与 $\alpha \in U$ 情形同样的公式.

对于上述的 α 和 $f(X)$, 由于 $\alpha = f(\pi)$, 从而 $\frac{f'(\pi)}{\alpha}$ 可以形式地写成 $\frac{1}{\alpha} \frac{d\alpha}{d\pi}$. 由于 $f'(\pi)/\alpha$ 不仅依赖于 α 而且还依赖于表示 α 的幂级数 $f(X)$ 的取法, 所以 $\frac{1}{\alpha} \frac{d\alpha}{d\pi}$ 不是正确的记号. 但是当

问题只涉及 $f(\pi)/\alpha$ 所在的 $\mathfrak{p}^{-1}/\mathfrak{d}$ 之剩余类的时候, 则不会引起混淆. 因此, 在今后不会产生误解的时候, 对于 k^\times 中的每个元素, 通常也把 $\mathfrak{p}^{-1}/\mathfrak{d}$ 中包含 $\delta_\pi(\alpha)$ 的剩余类写成

$$\frac{1}{\alpha} \frac{d\alpha}{d\pi}.$$

从而

$$\begin{aligned} \delta_\pi: k^\times &\rightarrow \mathfrak{p}^{-1}/\mathfrak{d}, \\ \alpha &\mapsto \frac{1}{\alpha} \frac{d\alpha}{d\pi} \bmod \mathfrak{d}. \end{aligned}$$

又如果 π_1 是 k 中另一个素元, 如上所述取 $\pi_1 = \omega(\pi)$, 则

$$\frac{d\pi_1}{d\pi} = \omega'(\pi)$$

是 U 中元素, 从而

$$\frac{1}{\alpha} \frac{d\alpha}{d\pi} \equiv \frac{1}{\alpha} \frac{d\alpha}{d\pi_1} \frac{d\pi_1}{d\pi} \bmod \mathfrak{d}, \quad \alpha \in k^\times.$$

即

$$\delta_\pi(\alpha) = \frac{d\pi_1}{d\pi} \delta_{\pi_1}(\alpha), \quad \alpha \in k^\times.$$

注记 形式上 $\frac{1}{\alpha} \frac{d\alpha}{d\pi}$ 等于 α 的对数微商 $\frac{d}{d\pi} \log \alpha$, 但是要注意,

当 k 的特征为 0 的时候, 如 § 8.1 所述, 对于 $U_1 = 1 + \mathfrak{p}$ 中元素 α 可以定义 $\log \alpha$, 并且 $\log \alpha$ 是 \mathfrak{o} 中元素, 从而

$$\log \alpha = g(\pi), \quad g(X) \in \mathfrak{o}_0[[X]].$$

于是又可定义 $g'(\pi) = \frac{d}{d\pi} \log \alpha$. 但是这个 $g'(\pi)$ 与上面的 $\frac{1}{\alpha} \frac{d\alpha}{d\pi}$ 对于 $\bmod \mathfrak{d}$ 不一定同余. 我们在下节将要叙述这样的例子.

§ 8.4 Artin-Hasse 公式

以下设 p 是任意奇素数, 考虑 \mathbb{Q}_p 的 p -分圆域

$$C_p = \mathbb{Q}_p(\zeta_p).$$

固定 W_p 的一个生成元 ζ , 于是 ζ 是 C_p 中的 p 次本原单位根. 令

$$\pi = 1 - \zeta,$$

则 π 显然是 $\mathbb{Z}_p[X]$ 的 Eisenstein 多项式

$$h(X) = \frac{1 - (1 - X)^p}{X} = X^{p-1} - pX^{p-2} + \cdots + p \quad (3)$$

的根, 从而 $C_p = \mathbb{Q}_p(\zeta) = \mathbb{Q}_p(\pi)$ 是 \mathbb{Q}_p 的 $p-1$ 次完全分歧扩张, 并且 π 是 C_p 的素元, 而且 $N_{C_p/\mathbb{Q}_p}(\pi) = p$. 这一切已经在 § 8.1 中作了更一般的说明. 由于 C_p/\mathbb{Q}_p 完全分歧, 我们可以对于

$$k_0 = \mathbb{Q}_p, \quad k = C_p = \mathbb{Q}_p(\zeta)$$

以及上面定义的 $\pi = 1 - \zeta$ 采用前节的结果. 设 v 和 $\mathfrak{f} = \mathfrak{o}/\mathfrak{p}$ 分别是 $k = C_p$ 的正规赋值和剩余类域, 由完全分歧性导致 \mathfrak{f} 是 p 元有限域, 即 $\mathfrak{f} = \mathbb{F}_p$, $q = p$, 并且 $v|_{\mathbb{Q}_p} = (p-1)v_p$, 其中 v_p 是 \mathbb{Q}_p 的 p -adic 赋值. 于是

$$v(p) = p-1, \quad p\mathfrak{o} = \mathfrak{p}^{p-1}.$$

从而 $h'(\pi) \equiv (p-1)\pi^{p-2} \pmod{\mathfrak{p}}$, 这就得到

$$\mathfrak{d} = (h'(\pi)) = \mathfrak{p}^{p-2},$$

于是作为 \mathfrak{o} -模有 $\mathfrak{p}^{-1}/\mathfrak{d} \cong \mathfrak{o}/\mathfrak{p}^{p-1} = \mathfrak{o}/p\mathfrak{o}$. $k = C_p$ 的单位群 U 的子群 U_i , $i \geq 0$ 为

$$U_0 = U, \quad U_i = 1 + \mathfrak{p}^i, \quad i \geq 1.$$

由定义和 $q = p$ 可知 U_i/U_{i+1} ($i \geq 1$) 均是 p 阶循环群. 从而由于 $\zeta \equiv 1 \pmod{\mathfrak{p}}$, $\zeta \not\equiv 1 \pmod{\mathfrak{p}^2}$ 可知

$$k^\times = \langle \pi \rangle \times U, \quad U = V \times U_1, \quad U_1 = W_p \times U_2.$$

但是 V 是 $p-1$ 阶循环群, 从而 $V \cong \mathbb{F}^\times$. 又由于

$$v|_{\mathbb{Q}_p} = (p-1)v_p$$

和 § 8.1 中的注记, 可知 \exp 和 \log 定义出互逆的同构:

$$\exp: \mathfrak{p}^2 \xrightarrow{\sim} U_2 = 1 + \mathfrak{p}^2, \quad \log: U_2 = 1 + \mathfrak{p}^2 \xrightarrow{\sim} \mathfrak{p}^2,$$

特别地,

$$\begin{aligned} \log(1 + \mathfrak{p}^2)^p &= p \log(1 + \mathfrak{p}^2) = p\mathfrak{p}^2 \\ &= \mathfrak{p}^{p+1} = \log(1 + \mathfrak{p}^{p+1}), \end{aligned}$$

从而得到

$$U_1^p = U_1^p = U_{p+1}.$$

对于 U_1 中每个元素 α 均可定义 $\log \alpha$. 由于

$$p \log \zeta = \log \zeta^p = \log 1 = 0,$$

从而

$$\log \zeta = 0.$$

于是得到正合序列

$$1 \rightarrow W_p \rightarrow U_1 \xrightarrow{\log} p^2 \rightarrow 1.$$

由 $U_1 = W_p \times U_2$ 可以看出这个正合序列是分裂的.

注记 由于 $\log \zeta = 0$, 从而 $\frac{d}{d\pi} \log \zeta = 0$. 但是另一方面,

由 $\zeta = 1 - \pi$ 可知 $\frac{1}{\zeta} \cdot \frac{d\zeta}{d\pi} = -\frac{1}{\zeta}$. 因此在这种情形下

$$\frac{d}{d\pi} \log \zeta \not\equiv \frac{1}{\zeta} \frac{d\zeta}{d\pi} \pmod{d}.$$

(参见前节末尾的注记.)

设 $T = T_{C_p/Q_p}$ 是从 $k = C_p$ 到 Q_p 的迹, 对于每个 $\alpha \in k^\times$, $\beta \in U_1 = 1 + p$, 定义 Q_p 中元素 $[\alpha, \beta]$ 为

$$[\alpha, \beta] = -\frac{1}{p} T \left(\zeta \frac{1}{\alpha} \frac{d\alpha}{d\pi} \log \beta \right).$$

$\frac{1}{\alpha} \frac{d\alpha}{d\pi}$ 作为 p^{-1}/d 的剩余类是确定的元素, 但是 $[\alpha, \beta]$ 不一定由 α, β 所唯一决定. 然而我们有如下的引理

引理 5 $[\alpha, \beta]$ 属于 Z_p , 并且它在 Z_p/pZ_p 中的剩余类由 α 和 β 所完全确定.

证明 首先注意有 $T(p) \subseteq pZ_p$ (参见 § 1.2 末尾的注记). 由于 $\frac{1}{\alpha} \frac{d\alpha}{d\pi} \in p^{-1}$, $\log \beta \in \log U_1 \subseteq p^2$, 从而

$$T \left(\zeta \frac{1}{\alpha} \frac{d\alpha}{d\pi} \log \beta \right) \in T(p^{-1}p^2) = T(p) \subseteq pZ_p.$$

从而 $[\alpha, \beta] \in Z_p$, 并且

$$T(\zeta \mathfrak{d} \log \beta) \subseteq T(\mathfrak{p}^{p-2} \mathfrak{p}^2) = T(\mathfrak{p} \mathfrak{p}) \subset \mathfrak{p}^2 \mathbf{Z}_p,$$

由此即证引理.

从 § 8.1 的叙述可知环 \mathbf{Z}_p 可以作用在有限 p 群 W_p 上, 由于 $\zeta^p = 1$, 从而由上引理可知

$$\zeta^{[\alpha, \beta]}, \alpha \in k^\times, \beta \in U_1$$

决定出 W_p 中唯一的元素, 并且

$$\delta_\pi: k^\times \rightarrow \mathfrak{p}^{-1}/\mathfrak{d},$$

$$\alpha \mapsto \frac{1}{\alpha} \frac{d\alpha}{d\pi} \bmod \mathfrak{d}$$

和

$$\log: U_1 \rightarrow \mathfrak{p}^2,$$

$$\beta \mapsto \log \beta$$

均是从乘法群到加法群的同态, 并且

$$\begin{aligned} [\alpha\alpha', \beta] &\equiv [\alpha, \beta] + [\alpha', \beta] \bmod \mathfrak{p}\mathbf{Z}_p, \\ [\alpha, \beta\beta'] &\equiv [\alpha, \beta] + [\alpha, \beta'] \bmod \mathfrak{p}\mathbf{Z}_p, \end{aligned} \quad (4)$$

从而 $\zeta^{[\alpha, \beta]}$ 对于 α 和 β 均是积性的.

现在对一些特别的 α, β 计算 $[\alpha, \beta]$ 的值. 为此首先证明以下的引理.

引理 6 设 n, a 为整数并且 $2 \leq 2p^a \leq n$, $n \neq p$, 则

$$\frac{1}{p^{a+1}} T(\zeta \pi^{n-1}) \equiv 0 \bmod p,$$

而当 $n = p(a = 0)$ 的时候,

$$\frac{1}{p} T(\zeta \pi^{p-1}) \equiv 1 \bmod p.$$

证明 首先若 $2 \leq n \leq p$, $a = 0$, 则

$$\frac{1}{p} T(\zeta \pi^{n-1}) = \frac{1}{p} \sum_{i=0}^{n-1} (-1)^i \binom{n-1}{i} T(\zeta^{i+1}).$$

因为当 $i+1 \leq n \leq p$ 时,

$$T(\zeta^{i+1}) = \begin{cases} -1, & i+1 < p, \\ p-1, & i+1 = p. \end{cases}$$

从而当 $n < p$ 时,

$$\begin{aligned}\frac{1}{p} T(\zeta \pi^{n-1}) &= -\frac{1}{p} \sum_{i=0}^{n-1} (-1)^i \binom{n-1}{i} \\ &= -\frac{1}{p} (1-1)^{n-1} = 0.\end{aligned}$$

当 $n = p$ 时,

$$\begin{aligned}\frac{1}{p} T(\zeta \pi^{p-1}) &= -\frac{1}{p} \sum_{i=0}^{p-1} (-1)^i \binom{p-1}{i} \\ &\quad + \frac{p}{p} = 1.\end{aligned}$$

最后设 $n > p$. 由于 $T(p) \subseteq p\mathbb{Z}_p$ 和

$$\frac{1}{p^{a+1}} \zeta \pi^{n-1} \in p^{n-1-(a+1)(p-1)},$$

从而只需证明 $n-1-(a+1)(p-1) > 0$. 当 $a=0$ 时这显然是对的. 而当 $a \geq 1$ 时

$$\begin{aligned}n-1-(a+1)(p-1) &\geq 2p^a-1-(a+1)(p-1) \\ &= 2p^a-a(p-1)-p \\ &\geq p^a-a(p-1) = (1+(p-1))^a-a(p-1) \\ &= (1+a(p-1)+\cdots)-a(p-1) > 0.\end{aligned}$$

更一般地, 对于任一自然数 $i \geq 1$, 记

$$\eta_i = 1 - \pi^i.$$

由于 $[U_i:U_{i+1}] = p$, 从而 U_i/U_{i+1} 是由 $\zeta = 1 - \pi = \eta_1$ 的剩余类所生成的, 而 U_i/U_{i+1} 是由 η_i 的剩余类所生成的.

引理 7 当 $i \geq 2$ 时,

$$[\pi, \eta_i] \equiv \begin{cases} 0 & \text{mod } p, \quad \text{当 } i \neq p \text{ 时,} \\ 1 & \text{mod } p, \quad \text{当 } i = p \text{ 时,} \end{cases}$$

并且对于任意 $i \geq 1$, 均有

$$[\eta_i, \eta_j] \equiv - \sum_{r+s=i} \frac{1}{s} \text{ mod } p.$$

其中右边求和是过满足条件 $ri + sj = p$ 的全部自然数 $r, s \geq 1$.

证明 首先由定义有

$$\begin{aligned}
[\pi, \eta_i] &= -\frac{1}{p} T\left(\zeta \log(1 - \pi^i)\right) \\
&= -\frac{1}{p} T\left(\zeta \sum_{j=1}^{\infty} \frac{\pi^{ij}}{j}\right) \\
&= \sum_{j=1}^{\infty} \frac{1}{p} \frac{1}{j} T(\zeta \pi^{ij-1}).
\end{aligned}$$

如果 $p \nmid s$, 则由 $j \geq 2$ 可知 $2 \leq 2p^a \leq sj$. 根据引理 6 可知当 $sj \neq p$ 时

$$\frac{1}{p} \frac{1}{j} T(\zeta \pi^{ij-1}) \equiv 0 \pmod{p}.$$

而当 $sj = p$ 时只需考虑 $j = p, s = 1, a = 0$ 的情形. 这时再由引理 6 可知

$$\frac{1}{p} \frac{1}{j} T(\zeta \pi^{ij-1}) = \frac{1}{p} T(\zeta \pi^{p-1}) \equiv 1 \pmod{p}.$$

由此即证实了关于 $[\pi, \eta_i]$ 的公式. 其次, 与上面同样地有

$$\begin{aligned}
[\eta, \eta_i] &= -\frac{1}{p} T\left(\zeta \frac{1 - \pi^{i+1}}{1 - \pi} \log(1 - \pi^i)\right) \\
&= -\frac{1}{p} T\left(\zeta i \sum_{r=1}^{\infty} \pi^{r-1} \sum_{j=1}^{\infty} \frac{1}{j} \pi^{rj}\right) \\
&= -\frac{1}{p} \sum_{r, j \geq 1} T\left(\frac{i}{j} \zeta \pi^{r+j-1}\right).
\end{aligned}$$

从而当 $p \nmid s$ 时, 如果 $2 \leq 2p^a \leq ri + sj$, 将引理 6 用于 $ri + sj \neq p$

的情形, 则

$$\frac{1}{p} T\left(\frac{i}{j} \zeta \pi^{r+j-1}\right) \equiv 0 \pmod{p}.$$

另一方面, 如果 $ri + sj = p, a = 0$, 由于 $1 \leq r, s < p$, 从而

$$\frac{1}{p} T\left(\frac{i}{j} \zeta \pi^{r+j-1}\right) = \frac{i}{s} \pmod{p}.$$

这就证明了引理.

注记 关于 $[\eta, \eta_i]$ 的同余式对于 $i \neq 1, \eta_i = \eta_{i-1} = \dots = \eta_1 = \zeta$ 不一定成立. 例如 $i = p-1$ 时, $[\eta_{p-1}, \eta_1] \equiv 0 \pmod{p}$, 而 $-\sum_{s=1}^{p-1} \zeta^s \equiv 1 \pmod{p}$.

今后我们主要考查 $k = C_p$ 的 p 次范剩余符号 $(\alpha, \beta)_p$. 为简单起见, 今后将 $(\alpha, \beta)_p$ 写成 (α, β) .

引理 8 $k(\sqrt[p]{\eta_p})$ 是 k 的 p 次不分歧扩张, 并且若以 φ 表示 k_{φ}/k 的 Frobenius 自同构, 则

$$(\sqrt[p]{\eta_p})^{\varphi-1} = \zeta.$$

证明 令 $k' = k(\sqrt[p]{\eta_p})$, $f = o/p'$ 为 k' 的剩余类域. 由于 $\zeta \in k$, 从而 k'/k 是 1 次或者 p 次循环扩张. 如果

$$\sqrt[p]{\eta_p} = 1 + \alpha\pi,$$

即

$$\alpha = (\sqrt[p]{\eta_p} - 1)/\pi,$$

则 α 显然满足

$$\alpha^p + \sum_{i=1}^{p-1} \binom{p}{i} \frac{\pi^i}{\pi^p} \alpha^i + 1 = 0.$$

由于 $v(p) = p-1$, 从而对于 $1 \leq i \leq p-1$ 我们有

$$\binom{p}{i} \pi^{i-p} \in o.$$

从而由 § 1.2, 引理 4 可知 $\alpha \in o$. 另一方面, 由于 $v(\pi) = 0$, 因此由 (3) 式得到 $\frac{p}{\pi^p} \equiv -1 \pmod{p}$. 再由上面的等式得到

$$\alpha^p - \alpha + 1 \equiv 0 \pmod{p'}.$$

但是 k 的剩余类域 f 是 p 元域 F_p , 并且 $X^p - X + 1$ 在 $F_p[X]$ 中是不可约的, 从而 $[f':f] \geq p$. 另一方面 $[k':k] \leq p$, 从而 $[k':k] = p$, $e = 1$, $f = p$, 即 k'/k 是 p 次不分歧扩张. 再由上面的同余式便得到

$$\alpha^p \equiv \alpha^p - \alpha + 1 \pmod{p'}.$$

从而

$$\begin{aligned} (\sqrt[p]{\eta_p})^{p-1} &= (1 + \pi\alpha^p)(1 + \pi\alpha)^{-1} \\ &= 1 + \pi(\alpha^p - \alpha) \bmod p^2 \\ &\equiv 1 - \pi \equiv \zeta \bmod p^2. \end{aligned}$$

显然 $(\sqrt[p]{\eta_p})^{p-1}$ 是 p 次单位根, 即属于 W_p , 而 k'/k 是不分歧扩张, 从而由上面所述即得到

$$(\sqrt[p]{\eta_p})^{p-1} \equiv \zeta \bmod p^2,$$

但是 $U_1 = W_p \times U_2$, 从而 $(\sqrt[p]{\eta_p})^{p-1} = \zeta$.

引理 9

$$(\pi, \eta_i) = \begin{cases} 1, & \text{当 } i \geq 1, i \neq p \text{ 时,} \\ \zeta, & \text{当 } i = p \text{ 时.} \end{cases}$$

证明 由于 (α, β) 是 k 上的符号, 从而

$$(\pi, \eta)^i = (\pi^i, \eta_i) = (\pi^i, 1 - \pi^i) = 1, i \geq 1.$$

但是 (π, η_i) 是 p 次单位根, 从而当 i 与 p 互素时, 由上式可得 $(\pi, \eta_i) = 1$. 特别当 $1 \leq i < p$ 时 $(\pi, \eta_i) = 1$. 由引理 8 知道 $k(\sqrt[p]{\eta_p})/k$ 是不分歧扩张, 从而 $\rho_k(\pi) | k(\sqrt[p]{\eta_p}) = \varphi$. 因此再用引理 8 便有

$$(\pi, \eta_p) = (\sqrt[p]{\eta_p})^{p-1} = \zeta.$$

最后若 $i \geq p+1$, 则 $\eta_i \in U_i \subseteq U_{r+1} = U_1^r$, 再由定理 4, ii) 即知 $(\pi, \eta_i) = 1$.

接下来考查 (η_i, η_j) , $i, j \geq 1$. 对于互素的自然数 $r, s \geq 1$, $(r, s) = 1$, 今后用 $\{r_0, s_0\}$ 表示满足 $rs_0 - sr_0 = 1$ 的任意一对整数. 这样的整数对 $\{r_0, s_0\}$ 一定存在, 并且如果 $\{r'_0, s'_0\}$ 也满足 $rs'_0 - sr'_0 = 1$, 则

$$r'_0 = r_0 + ar, s'_0 = s_0 + as, a \in \mathbb{Z}.$$

从而

$$r'_0 i + s'_0 j = r_0 i + s_0 j + a(r_i + s_j).$$

正如在引理 8 中所指出的, 对于任意

$$i \geq 1, (\pi, \eta_i)^r = (\pi^r, \eta_i) = 1,$$

于是由上式给出

$$(\pi, \eta_{r_i+s_i})^{r'_0+i'+s'_0} = (\pi, \eta_{r_i+s_i})^{r_0^i+s_0^i}.$$

换句话说, $(\pi, \eta_{r_i+s_i})^{r_0^i+s_0^i}$ 与 $\{r_0, s_0\}$ 的选取方法无关. 进而, 当 $r_i + s_i \geq r + s$ 时除了有限对 $\{r, s\}$ 之外均有 $\eta_{r_i+s_i} \in U_2^p$, 从而除有限对 $\{r, s\}$ 之外均有 $(\pi, \eta_{r_i+s_i}) = 1$. 注意上述各种事实便有如下引理.

引理 10 对于任意的 $i, j \geq 1$,

$$(\eta_i, \eta_j) = \prod_{r,s} (\pi, \eta_{r_i+s_i})^{r_0^i+s_0^i}.$$

其中右边乘积是过全部互素自然数对 $\{r, s\}$, 而 $\{r_0, s_0\}$ 如上所述.

证明 将等式右边写成

$$\Pi_{i,j} = \prod_{r,s} (\pi, \eta_{r_i+s_i})^{r_0^i+s_0^i}, \quad i, j \geq 1.$$

由上面所述知道这是有限乘积并且其值与 $\{r_0, s_0\}$ 的取法无关. 我们先证明两个等式:

$$(\eta_i, \eta_j) = (\eta_i, \eta_{i+j})(\eta_{i+j}, \eta_j)(\pi, \eta_{i+j})^j, \quad (5)$$

$$\Pi_{i,j} = \Pi_{i,i+j} \Pi_{i+j,j} (\pi, \eta_{i+j})^j. \quad (6)$$

由于 $p > 2$, 对于每个 $\alpha \in k^\times$, 均有

$$(-1, \alpha) = ((-1)^p, \alpha) = 1.$$

从而再利用

$$\eta_i + \pi^i \eta_j = \eta_{i+j}$$

和 § 8.2, 引理 1, 可得

$$(\eta_i, \pi^i \eta_j) = (\eta_i, \eta_{i+j})(\eta_{i+j}, \pi^i \eta_j).$$

但是 $(\eta_i, \pi^i) = 1$, $(\eta_{i+j}, \pi^i) = (\eta_{i+j}, \pi^j)^{-1} = (\pi, \eta_{i+j})^j$, 由此即得到(5)式. 其次我们分别考查乘积 $\Pi_{i,j}$ 中 $r = s$, $r > s$, 和 $r < s$ 三种情况. 由于 $(r, s) = 1$, 从而 $r = s$ 时只有 $r = s = 1$ 的情形. 这时取 $r_0 = 0$, $s_0 = 1$, 则

$$(\pi, \eta_{r_i+s_i})^{r_0^i+s_0^i} = (\pi, \eta_{i+j})^j.$$

如果 $r > s$, 令 $r' = r - s$, $s' = s$. 即 $r = r' + s'$, $s = s'$, 则

$r', s' \geq 1, (r, s) = 1$. 映射 $\{r, s\} \mapsto \{r', s'\}$ 是从集合 $\{\{r, s\} | r, s \text{ 为自然数}, r > s, (r, s) = 1\}$ 到集合 $\{\{r', s'\} | r', s' \text{ 为自然数}, (r', s') = 1\}$ 之上的 1-1 对应. 并且

$$\begin{aligned} (\pi, \eta_{ri+s'})^{r_0'+s_0'} &= (\pi, \eta_{r'+s'(i+j)})^{r_0's_0'+s_0'(i+j)}, \\ r's_0 - s'(r_0 - s_0) &= (r' + s')s_0 - s'r_0 \\ &= rs_0 - sr_0 = 1, \end{aligned}$$

从而乘积 $\Pi_{i,j}$ 中满足 $r > s$ 诸项之积是 $\Pi_{i+j,i}$. 同样地, 乘积 $\Pi_{i,j}$ 中满足 $r < s$ 诸项之积是 $\Pi_{i,j+i}$. 这就证明了(6)式.

令

$$q_{i,j} = (\eta_i, \eta_j) / \Pi_{i,j}, \quad i, j \geq 1.$$

如果 $i + j > 2p$, 则 $i \geq p + 1$ 或者 $j \geq p + 1$. 从而

$$\eta_i \in U_{p+1} = U_2^p$$

或者 $\eta_j \in U_{p+1} = U_2^p$, 因此 $(\eta_i, \eta_j) = 1$. 又由于

$$\eta_{ri+s'} \in U_{p+1} = U_2^p,$$

可知 $(\pi, \eta_{ri+s'}) = 1, \Pi_{i,j} = 1$. 因此

$$q_{i,j} = 1 \quad (\text{当 } i + j > 2p \text{ 时}).$$

将(5)式两边分别除以(6)式两边, 便得到

$$q_{i,j} = q_{i,i+j} q_{i+j,i}, \quad i, j \geq 1.$$

然后对于 $i + j$ 使用归纳法(但是从 n 到 $n - 1$ 归纳), 可知 $q_{i,j} = 1$. 从而对于任意 $i, j \geq 1$ 均有 $(\eta_i, \eta_j) = \Pi_{i,j}$, 这就证明了引理.

引理 11 对于任意 $i, j \geq 1$, 均有

$$(\eta_i, \eta_j) = \prod_{r,s} \zeta^{-ir/s},$$

其中右边乘积过满足 $ri + sj = p$ 的全部自然数对 (r, s)

证明 由引理 9 可知在引理 10 右边乘积中:

$$(\pi, \eta_{ri+s'}) = \begin{cases} 1, & \text{如果 } ri + sj \neq p, \\ \zeta, & \text{如果 } ri + sj = p. \end{cases}$$

并且当 $ri + sj = p$ 时, $1 \leq i, j, r, s < p$, 并且

$$j \equiv -ri/s \pmod{p},$$

从而

$$\begin{aligned} r_0 i + s_0 j &\equiv r_0 i - s_0 \frac{r i^2}{s} \\ &\equiv (r_0 s - s_0 r) \frac{1}{s} \equiv -\frac{1}{s} \pmod{p}. \end{aligned}$$

然后由引理 10 立刻得到本引理的等式.

有了以上的准备, 现在不难达到我们的目标, 即证明 Artin-Hasse 公式. 让我们再叙述一下已经给出的各种定义: p 是奇素数, $C_p = \mathbb{Q}_p(W_p)$ 是 \mathbb{Q}_p 的 p 分圆域, ζ 是 C_p 中 p 次本原单位根, $\pi = 1 - \zeta$ 是 C_p 的素元, \mathfrak{p} 是 C_p 的极大理想, $(\alpha, \beta)_p$ 是 C_p 上的 p 次范剩余符号. 最后令

$$[\alpha, \beta] = -\frac{1}{p} T \left(\zeta \frac{1}{\alpha} \frac{d\alpha}{dx} \log \beta \right),$$

$$\alpha \in k^\times, \beta \in U_1 = 1 + \mathfrak{p},$$

其中 T 是 C_p/\mathbb{Q}_p 的迹, 而 $[\alpha, \beta]$ 的值为 \mathbb{Z}_p 中元素并且是 $\pmod{p\mathbb{Z}_p}$ 确定的.

定理 7 (Artin-Hasse). 对于任意元素 $\alpha \in C_p^\times$ 和 $\beta \in 1 + \mathfrak{p}^2$, 均有

$$(\alpha, \beta)_p = \zeta^{[\alpha, \beta]}.$$

证明 上式左边是 C_p 上的符号, 从而对于 α 和 β 是积性的, 由 (4) 式知右边同样对于 α 和 β 是积性的. 此外, 两边均是 p 次单位根, 从而如果 $\alpha \in U_{p+1} = U_1^\times$ 或者 $\beta \in U_{p+1} = U_1^\times$, 则两边的值均是 1. 因此只需对于 α 和 β 分别为 k^\times/U_{p+1} 和 U_1/U_{p+1} 的剩余类代表元时证明等式即可. 如前所述我们有

$$C_p^\times = \langle \pi \rangle \times V \times U_1.$$

由于 V 是 $p-1$ 阶循环群, V 中元素均满足 $v = v^p$, 从而由上所述我们有

$$(v, \beta)_p = \zeta^{[v, \beta]} = 1.$$

另一方面, $U_i/U_{i+1} (i \geq 1)$ 是由 η_i 的剩余类生成的, 从而只需对于

$$\alpha = \pi, \eta_i (i \geq 1), \beta = \eta_j (j \geq 2)$$

证明定理中的等式即可。但是由引理 7 和 9 可知

$$(\pi, \eta) = \zeta^{[x, \eta]}, j \geq 2,$$

又由引理 7 和 11 可知

$$(\eta_i, \eta_j) = \zeta^{[\eta_i, \eta_j]}, i \geq 1, j \geq 2,$$

由此即证定理。

定理 8

$$(\alpha, \beta)_p = \zeta^{-\frac{1}{p} T\left(\zeta \frac{d\alpha}{d\pi} \log \beta\right)}, \alpha \in 1 + \mathfrak{p}, \beta \in 1 + \mathfrak{p}^2,$$

$$(\pi, \beta)_p = \zeta^{-\frac{1}{p} T\left(\frac{\zeta}{\pi} \log \beta\right)}, \beta \in 1 + \mathfrak{p},$$

$$(\zeta, \beta)_p = \zeta^{\frac{1}{p} T(\log \beta)}, \beta \in 1 + \mathfrak{p}.$$

证明 第一等式是定理 7 的特殊情形。令 $\alpha = \pi$, 则

$$\frac{1}{\alpha} \frac{d\alpha}{d\pi} = \frac{1}{\pi},$$

又对于 $\alpha = \zeta = 1 - \pi$ 有 $\frac{1}{\alpha} \frac{d\alpha}{d\pi} = -\frac{1}{\zeta}$, 从而若 β 是

$$U_2 = 1 + \mathfrak{p}^2$$

中元素, 则第二、三式也是定理 7 的特例。最后由于

$$1 + \mathfrak{p} = U_1 = W_p \times U_2,$$

从而只需再对 $\beta = \zeta$ 的情形证明后两个公式即可。但是这时,

$$(\pi, \zeta)_p = (1 - \zeta, \zeta)_p = 1,$$

$$(\zeta, \zeta)_p = (\zeta, -\zeta)_p (\zeta, -1)_p = 1.$$

再由 $\log \zeta = 0$ 即证明了定理。

于是, 定理 8 很容易地由定理 7 推导出来, 反过来, 也可以由定理 8 直接推出定理 7。因为 $C_p^\times = \langle \pi \rangle \times V \times U_1$ 以及用公式

$$(\alpha, \beta)_p (\beta, \alpha)_p = 1, (\nu, \beta)_p = (\alpha, \nu)_p = 1,$$

$$\alpha, \beta \in C_p^\times, \nu \in V,$$

可知对于任意元素 $\alpha, \beta \in C_p^\times$, 均可由定理 8 计算 $(\alpha, \beta)_p$ 。在这个意义上, 我们把定理 7 或者定理 8 中的公式叫作范剩余符号 $(\alpha, \beta)_p$ 的显公式。

更一般地, 对于 $\mathbb{Q}_p (p \geq 2)$ 上的 p^n 分圆域的 p^n 次范剩余

符号 Artin-Hasse [2] 证明了与定理 8 的第二、三公式同样的等式¹⁾. 对于同样的情形, 岩澤和工藤将定理 7 中的公式加以推广. 所有这些结果都是采用自 Eisenstein 以来的传统计算方法得出的. 但是最近 Wiles^[15] 应用第七章中所讲的形式群, 不但对于 \mathbb{Q}_p 的分圆域, 而且对于特征为 0 的 p 局部域的任意有限 Abel 扩域均得出同样的结果, 并且方法很简洁. 这是关于椭圆曲线上有理点的 Coates Wiles 理论中的重要结果之一. 我们这里作为在局部域中进行计算的一个实例, 只介绍了古典的证明.

1) 关于定理 8 的结果在 Artin-Hasse 的文章 [2] 中写成定理 7 的形式, 随后二人又分别发表.

附录 局部域的 Brauer 群

现在我们简单讲述一下在正文中未能触及的关于局部域上的 Brauer 群, Brauer 群定义为 Galois 群的上同调群,从而首先对于上同调群的有关事项作一(最低限度的)介绍,然后定义 Brauer 群,特别是决定局部域上 Brauer 群的结构,详情请参照河田[8], Serre [11] 等。

§ A.1 一般的上同调群

设 G 是任意群, G 作用在 Abel 群 A 上,从而 A 是 G -模(但在以后应用中, A 的运算记为乘法). 以 $C^1 = C^1(G, A)$ 表示从 G 到 A 的映射

$$f: G \rightarrow A$$

全体. 而以 $Z^1 = Z^1(G, A)$ 表示其中满足

$$\sigma f(\tau) = f(\sigma\tau) + f(\sigma) = 0 \quad (\text{对任意 } \sigma, \tau \in G) \quad (1)$$

的映射 f 的全体. 在 C^1 中定义加法 $f + g$ 为:

$$(f + g)(\sigma) = f(\sigma) + g(\sigma),$$

从而 C^1 为 Abel 群, 而 Z^1 是它的子群. 此外, 对于 A 中一个固定的元素 a , 令

$$f_a(\sigma) = \sigma a - a, \quad \sigma \in G,$$

则 $f_a: G \rightarrow a$ 属于 Z^1 , 这种 $f_a(a \in A)$ 全体 $B^1 = B^1(G, A)$ 是 Z^1 的子群. 商群

$$H^1(G, A) = Z^1(G, A)/B^1(G, A)$$

叫作 G 的以 A 为系数(或者叫取值于 A)的一维上同调群. 类似地, 以 $C^2 = C^2(G, A)$ 表示从 $G^2 = G \times G$ 到 A 的映射全体组成的 Abel 群, 而其中满足

$$\begin{aligned} \sigma f(\tau, \rho) - f(\sigma\tau, \rho) + f(\sigma, \tau\rho) - f(\sigma, \tau) &= 0, \\ \sigma, \tau, \rho &\in G \end{aligned} \quad (2)$$

的全部 $f: G^2 \rightarrow A$ 形成 C^2 的子群并且记成 $Z^2 = Z^2(G, A)$. 对于 $C^1(G, A)$ 中每个元素 $f: G \rightarrow A$, 令

$$\partial f(\sigma, \tau) = \sigma f(\tau) - f(\sigma\tau) + f(\sigma), \quad \sigma, \tau \in G.$$

则 $\partial f: G^2 \rightarrow A$ 属于 Z^2 , 这种 $\partial f (f \in C^1)$ 全体 $B^2 = B^2(G, A)$ 是 Z^2 的子群. 而商群

$$H^2(G, A) = Z^2(G, A) / B^2(G, A)$$

叫作 G 的系数属于 A 的二维上同调群. 一般地, 对于任意 $n \geq 0$, 可以统一的定义出 n 维上同调群 $H^n(G, A)$. 由于今后不需要从而略去. 只是注意 Z^1 是由 C^1 中满足 $\partial f = 0$ 的元素 f 所组成的集合.

设 G' 为群而 A' 为 G' -模, 并且存在同态

$$\gamma: G' \rightarrow G, \quad \alpha: A \rightarrow A'.$$

对于每个 $\sigma' \in G'$, $a \in A$, 如果满足

$$\alpha(\gamma(\sigma')a) = \sigma'\alpha(a), \quad (3)$$

则将 $\lambda = (\gamma, \alpha)$ 叫作从 (G, A) 到 (G', A') 的态射 (morphism), 并且写成

$$\lambda: (G, A) \rightarrow (G', A').$$

这时对于 $C^1(G, A)$ 中每个元素 $f: G \rightarrow A$, 以 f' 表示合成映射

$$G' \xrightarrow{\gamma} G \xrightarrow{f} A \xrightarrow{\alpha} A',$$

$f \mapsto f'$ 显然定义了同态 $C^1(G, A) \rightarrow C^1(G', A')$, 而由上述条件 (3) 可知这个同态将 $Z^1(G, A)$, $B^1(G, A)$ 分别映到 $Z^1(G', A')$ 和 $B^1(G', A')$ 之中. 从而 $\lambda = (\gamma, \alpha)$ 诱导出上同调群的同态

$$H^1(G, A) \rightarrow H^1(G', A').$$

完全同样地定义同态 $C^2(G, A) \rightarrow C^2(G', A')$, 从而诱导出

$$H^2(G, A) \rightarrow H^2(G', A').$$

(一般地也可得到 $H^n(G, A) \rightarrow H^n(G', A')$, $n \geq 0$.) 特别若 H

是 G 的任意子群, 每个 G -模 A 也看成是 H -模, 令 $i: H \rightarrow G$ 是自然单射, $id: A \rightarrow A$ 是恒等映射, 则在上述意义下定义出

$$(i, id): (G, A) \rightarrow (H, A),$$

由此得到的同态

$$res: H^1(G, A) \rightarrow H^1(H, A),$$

$$H^2(G, A) \rightarrow H^2(H, A)$$

叫作限制映射 (restriction). 又若 H 是 G 的正规子群, 令

$$A^H = \{a \in A \mid \omega a = a, \text{ 对于每个 } \omega \in H\},$$

这显然是 G/H 模. 令 $\gamma: G \rightarrow G/H$ 是自然满射, $i: A^H \rightarrow A$ 是自然单射, 则在上述意义下又定义出态射

$$(\gamma, i): (G/H, A^H) \rightarrow (G, A),$$

由此得到的同态

$$inf: H^1(G/H, A^H) \rightarrow H^1(G, A),$$

$$H^2(G/H, A^H) \rightarrow H^2(G, A)$$

叫作膨胀映射 (inflation).

引理 1 如果 H 是 G 的正规子群, 则

$$0 \rightarrow H^1(G/H, A^H) \xrightarrow{inf} H^1(G, A) \xrightarrow{res} H^1(H, A)$$

是正合序列, 又若 $H^1(H, A) = 0$, 则

$$0 \rightarrow H^2(G/H, A^H) \xrightarrow{inf} H^2(G, A) \xrightarrow{res} H^2(H, A)$$

是正合序列

现在考查 G 是 n 阶循环群的情形. 固定 G 的一个生成元 ρ :

$$G = \{1, \rho, \dots, \rho^{n-1}\}, \rho^n = 1.$$

与上面同样地, 令 $A^G = \{a \in A \mid \sigma a = a, \text{ 对于每个 } \sigma \in G\}$

$$= \{a \in A \mid (\rho - 1)a = 0\}.$$

又令 $N(A) = (1 + \rho + \dots + \rho^{n-1})A$, 则显然有

$$N(A) \subseteq A^G \subseteq A.$$

对于任意元素 $a \in A^G$ 和 $0 \leq i, j < n$, 定义 $f: G^2 \rightarrow A$ 为

$$f(\rho^i, \rho^j) = \begin{cases} 1, & \text{如果 } i+j < n, \\ a, & \text{如果 } i+j \geq n, \end{cases}$$

可直接验证 $f \in Z^2 = Z^2(G, A)$, 以 c_a 表示 $Z^2/B^2 = H^2(G, A)$ 中包含 f 的陪集.

引理 2 $a \mapsto c_a$ 诱导出同构

$$A^G/N(A) \cong H^2(G, A).$$

类似地, 令

$$A_N = \{a \in A \mid (1 + \rho + \cdots + \rho^{n-1})a = 0\},$$

则对于每个 $a \in A_N$, 存在 $f \in Z^1 = Z^1(G, A)$ 使得 $f(\rho) = a$, 熟知由 $a \mapsto f \bmod B^1$ 诱导出同构

$$A_N/(1 - \rho)A \cong H^1(G, A).$$

设 H 是上述循环群 $G = \langle \rho \rangle$ 的子群, 令 $[G: H] = m$, 则 G/H 是由 $\bar{\rho} = \rho H$ 生成的 m 阶循环群. 注意 $A^G = (A^H)^{G/H}$, 从而由引理 2 可知 $\bar{\rho}$ 定义出同构

$$A^G/(1 + \bar{\rho} + \cdots + \bar{\rho}^{m-1})A^H \cong H^2(G/H, A^H).$$

对于 $b \in A^H$, 则

$$(1 + \rho^m + \rho^{2m} + \cdots + \rho^{(n/m-1)m})b = \sum_{i=0}^{n/m-1} b,$$

$$\frac{n}{m}(1 + \rho + \cdots + \rho^{m-1})b = (1 + \rho + \cdots + \rho^{n-1})b,$$

从而 A^G 的自同态 $a \mapsto \sum_{i=0}^{n/m-1} a$ 诱导出

$$\begin{aligned} \frac{n}{m}: A^G/(1 + \bar{\rho} + \cdots + \bar{\rho}^{m-1})A^H \\ \rightarrow A^G/(1 + \rho + \cdots + \rho^{n-1})A. \end{aligned}$$

引理 3 图表

$$\begin{array}{ccc} A^G/(1 + \bar{\rho} + \cdots + \bar{\rho}^{m-1})A^H & \cong & H^2(G/H, A^H) \\ \downarrow n/m & & \downarrow \text{inf} \\ A^G/(1 + \rho + \cdots + \rho^{n-1})A & \cong & H^2(G, A) \end{array}$$

是交换的. 其中二行分别是由 ρ 和 $\bar{\rho} = \rho H$ 所定义的同构.

上述三个引理是我们今后所需要的关于上同调群的全部结果. 引理 1 的前半部分和引理 2, 3 (以及引理 2 后面的注记) 均可由上同调群的定义比较简单地证明出来. 引理 1 的后半部分也

可以直接计算出来,或者利用上同调群的函子 (functor) 性质容易将它归结成引理的前半部分. 所有这些证明均略去¹⁾,但是要特别注意,引理 2 和其后的注记中所采用的同构均依赖于 G 的生成元 ρ 的选取方法.

设群 P 包含正规子群 A , 并且 A 是 G -模, 如果存在同构 $\varphi: G \cong P/A$, 由于 A 是 Abel 群, P/A 自然地作用在 A 上²⁾, 从而通过 φ 使得 G 又作用于 A 上. 如果这个作用与 G 在作为 G -模的 A 上本来的作用一致的话, 我们便称 (P, φ) 是 G -模 A 在 G 上的扩张 (extension). 对于 G 中每个元素 σ , 在 P/A 的陪集 $\varphi(\sigma)$ 中选定一个元素 $u_\sigma \in P$, 则上述条件可写为

$$u_\sigma a u_\sigma^{-1} = \sigma a (= a^\sigma), \quad a \in A.$$

如果 σ 和 τ 为 G 中任意元素, 由于 $u_\sigma u_\tau \equiv u_{\sigma\tau} \pmod{A}$, 从而存在元素 $a_{\sigma,\tau} \in A$ 满足

$$u_\sigma u_\tau = a_{\sigma,\tau} u_{\sigma\tau}.$$

而由 $(u_\sigma u_\tau) u_\rho = u_\sigma (u_\tau u_\rho)$ 得到

$$a_{\sigma,\tau} a_{\sigma\tau,\rho} = a_{\tau,\rho}^\sigma a_{\sigma,\tau\rho}, \quad \sigma, \tau, \rho \in G.$$

于是若令

$$f(\sigma, \tau) = a_{\sigma,\tau},$$

对于 $f: G^2 \rightarrow A$ 采用加法记号, 便有

$$f(\sigma, \tau) + f(\sigma\tau, \rho) = \sigma f(\tau, \rho) + f(\sigma, \tau\rho).$$

换句话说, f 属于 $Z^2 = Z^2(G, A)$. 如果改变 $\varphi(\sigma)$ 的代表元 u_σ , 则上面的 $f(\sigma, \tau)$ 也改变, 但是 $H^2(G, A) = Z^2/B^2$ 中包含 f 的陪集 c 不变. 从而 (P, φ) 唯一地决定出 $H^2(G, A)$ 中元素 c . 进而, 我们可以证明, 适当地 (自然地) 定义从扩张 (P_1, φ_1) 到扩张 (P_2, φ_2) 的同构 $(P_1, \varphi_1) \cong (P_2, \varphi_2)$, 使得

$$(P, \varphi) \mapsto c$$

是从 (P, φ) 的同构类的集合到 $H^2(G, A)$ 之上的一一对应. $H^2(G, A)$ 与群的扩张理论的这种关系是很早就知道的, 而对于

1) 例如参见 Serre [1.], 第七章 § 6.

2) P/A 在 A 上的自然作用是 $\bar{\sigma}(a) = \sigma a \sigma^{-1}$ ($\sigma \in P, \bar{\sigma} = \sigma \pmod{A}$). 译者注

任意 $n \geq 0$ 的 $H^n(G, A)$ 可以看成是它的推广. 此外还要注意, 如果使用 (P, φ) 和 $H^2(G, A)$ 之间的上述关系, 可以非常自然地证明出引理 2.

§ A.2 Galois 群的上同调群

设 K 是域 F 的 Galois 扩域, $G = \text{Gal}(K/F)$ 为它的 Galois 群, 则 G 显然作用在 K 的乘法群 K^\times 上, 从而由上节可定义 $H^1(G, K^\times)$ 和 $H^2(G, K^\times)$. Galois 群的上同调理论便是研究与这两个群只有少许差别的上同调群 $H^1(K/F)$ 和 $H^2(K/F)$. 现在来说明这件事. Galois 群 G 对于 Krull 拓扑是全不连通的紧群, 即是射影有限群. 另一方面, 将 K 的乘法群 K^\times 赋以离散拓扑, 对于这些拓扑, 以 $C_0^1(G, K^\times)$ 表示全体连续映射 $f: G \rightarrow K^\times$. 于是 $C_0^1(G, K^\times)$ 是 $C^1(G, K^\times)$ 的子群. 令

$$Z_0^1(G, K^\times) = Z^1(G, K^\times) \cap C_0^1(G, K^\times),$$

不难看出 $B^1(G, K^\times) \subseteq Z_0^1(G, K^\times)$. 定义它的商群为

$$H^1(K/F) = Z_0^1(G, K^\times) / B^1(G, K^\times).$$

类似地, 以 $C_0^2(G, K)$ 表示全体连续映射 $G^2 = G \times G \rightarrow K^\times$, $Z_0^2(G, K^\times) = Z^2(G, K^\times) \cap C_0^2(G, K^\times)$. 又令

$$B_0^2(G, K^\times) = \{\partial f \mid f \in C_0^1(G, K^\times)\},$$

它是 $Z_0^2(G, K^\times)$ 的子群. 定义商群

$$H^2(K/F) = Z_0^2(G, K^\times) / B_0^2(G, K^\times).$$

因而 $H^1(K/F)$ 和 $H^2(K/F)$ 是考虑了拓扑的 Galois 群

$$G = \text{Gal}(K/F)$$

的上同调群. 如果 K/F 是有限扩张, 则 G 是有限群, 从而

$$H^1(K/F) = H^1(G, K^\times), \quad H^2(K/F) = H^2(G, K^\times).$$

进而, 如果 E 是 K/F 的中间域, 则 $H = \text{Gal}(K/E)$ 是

$$G = \text{Gal}(K/F)$$

的闭子群. 由定义有

$$H^1(K/E) = Z_0^1(H, K^\times) / B^1(H, K^\times),$$

$$H^p(K, E) = Z_0^p(H, K^*) / B_0^p(H, K^*).$$

与不考虑拓扑的情形一样,可以定义限制映射

$$\text{res}: H^p(K/F) \rightarrow H^p(K/E), \quad H^p(K/F) \rightarrow H^p(K/E).$$

特别若 E/F 是 Galois 扩张,则还可定义膨胀映射

$$\text{inf}: H^p(E/F) \rightarrow H^p(K/F), \quad H^p(E/F) \rightarrow H^p(K/F).$$

现在设 $\{K_i\}(i \in I)$ 是包含在 K 中的一族 F 的有限 Galois 扩域,并且满足

$$K = \bigcup_i K_i. \quad (4)$$

例如包含在 K 中的全部 F 上有限 Galois 扩域就具有这样的性质. 令 $G_i = \text{Gal}(K_i/F)$, $i \in I$. 如果 $F \subset K_i \subseteq K_j$, $i, j \in I$, 则可定义自然的

$$\text{满射 } \gamma_{ij}: G_i \rightarrow G_j, \text{ 单射 } \alpha_{ij}: K_i^* \rightarrow K_j^*.$$

从而有上节意义下的态射

$$\lambda_{ij} = (\gamma_{ij}, \alpha_{ij}): (G_i, K_i^*) \rightarrow (G_j, K_j^*).$$

从而 γ_{ij} 诱导出同态

$$H^p(G_i, K_i^*) \rightarrow H^p(G_j, K_j^*), \quad H^p(G_i, K_i^*) \rightarrow H^p(G_j, K_j^*).$$

引理 4

$$H^p(K/F) = \varinjlim H^p(G_i, K_i^*), \quad H^p(K/F) = \varinjlim H^p(G_i, K_i^*).$$

其中右边是对于 $K_i \subseteq K_j$, $i, j \in I$ 由上面同态所给出的归纳极限.

证明 由于 $G = \text{Gal}(K/F)$ 是全不连通的紧群,从而由 G 到离散空间 K^* 的连续映射 $f: G \rightarrow K^*$ 只取有限个值. 因此在假定 (4) 之下可以适当地选取 K_i 和 $g: G_i \rightarrow K_i^*$, 使得 f 可以表示成下面的合成映射.

$$G \rightarrow G_i \xrightarrow{g} K_i^* \rightarrow K^*.$$

其中 $G \rightarrow G_i$ 和 $K_i^* \rightarrow K^*$ 分别是由 $F \subseteq K_i \subseteq K$ 产生的自然满射和自然单射. 从上节可知 λ_{ij} 定义出:

$$C^1(G_i, K_i^*) \rightarrow C^1(G_j, K_j^*),$$

再由上所述即知

$$C_i^1(G, K^\times) = \varinjlim C^1(G_i, K_i^\times).$$

对于子群同样有

$$Z_i^1(G, K^\times) = \varinjlim C^1(G, K_i^\times),$$

$$B^1(G, K^\times) = \varinjlim B^1(G, K_i^\times).$$

由于归纳极限保持正合序列,从而对于 K_i 定义的正合序列

$$0 \rightarrow B^1(G_i, K_i^\times) \rightarrow C^1(G_i, K_i^\times) \rightarrow H^1(G_i, K_i^\times) \rightarrow 0$$

取极限即得到正合序列

$$0 \rightarrow B^1(G, K^\times) \rightarrow C^1(G, K^\times) \rightarrow \varinjlim H^1(G_i, K_i^\times) \rightarrow 0.$$

于是

$$H^1(K/F) = \varinjlim H^1(G_i, K_i^\times).$$

对于 $H^2(K/F)$ 也可完全同样地证明.

定理 1 对于任意的 Galois 扩张 K/F , 均有

$$H^i(K/F) = 0.$$

证明 对于有限 Galois 扩张 K/F 我们有 $H^i(G_i, K_i^\times) = 0$, 这是 Galois 理论的一个熟知的基本定理. 再由上一引理即得

$$H^i(K/F) = \varinjlim H^i(G_i, K_i^\times) = 0.$$

引理 5 设 E 是 K/F 的中间域, 并且 E/F 是 Galois 扩张, 则

$$0 \rightarrow H^2(E/F) \xrightarrow{\text{inf}} H^2(K/F) \xrightarrow{\text{res}} H^2(K/E)$$

是正合序列.

证明 $\{K_i\}$, $i \in I$ 如前所述, 令

$$E_i = E \cap K_i, \quad H_i = \text{Gal}(K_i/E_i),$$

对于有限 Galois 扩张 K_i/F , $H^2(K_i/F)$ 与不考虑拓扑的上同调群 $H^2(G, K_i^\times)$ 是一致的, 由 $H^2(K_i/E_i) = 0$ 和引理 1 可知

$$0 \rightarrow H^2(E_i/F) \xrightarrow{\text{inf}} H^2(K_i/F) \xrightarrow{\text{res}} H^2(K_i/E_i)$$

是正合序列. 取归纳极限再应用引理 4 即得到正合序列

$$0 \rightarrow H^2(E/F) \rightarrow H^2(K/F) \rightarrow \varinjlim H^2(K_i/E_i).$$

采用与引理 4 的证明同样的考虑方法 (但是要复杂一些), 利用

$K_i \subset K$, 时的态射 $(H_i, K_i^\times) \rightarrow (H, K^\times)$, 可以证明

$$C_0^2(\text{Gal}(K/E), K^\times) = \varinjlim C^2(H_i, K_i^\times),$$

从而得到

$$H^2(K/E) = \varinjlim H^2(K_i/E_i).$$

另一方面, 不难看出上面的 $H^2(E/F) \rightarrow H^2(K/F)$ 和

$$H^2(K, F) \rightarrow \varinjlim H^2(K_i/E_i) = H^2(K/E)$$

分别与膨胀映射和限制映射一致, 从而证明了引理.

由引理 5 可知 $\text{inf}: H^2(E/F) \rightarrow H^2(K/F)$ 必是单射, 并且可以将它等同于 $\text{res}: H^2(K/F) \rightarrow H^2(K/E)$ 的核. 即可看成

$$H^2(E/F) \subset H^2(K/F).$$

特别对于先前的 $\{K_i\}$ 我们有 $H^2(K_i/F) \subset H^2(K/F)$, 从而

$$H^2(K/F) = \varinjlim H^2(K_i/F) = \bigcup_i H^2(K_i/F).$$

从而对于一般的 Galois 扩张 K/F , $H^2(K/F)$ 是对于有限 Galois 扩张 K_i/F 计算出来的 $H^2(K_i/F) = H^2(G_i, K_i^\times)$ 之并集合.

注记 对于不考虑拓扑的上同调群 $H^2(G, K^\times)$, 上述结果不成立. 这就是为什么 Galois 群的上同调理论要将 $H^2(G, K^\times)$ 改成 $H^2(K/F)$.

设 Ω_F 是域 F 的最大 Galois 扩域, 即包含在 F 的代数闭包 Ω 之中的 F 的最大可分扩域, 我们将 $H^2(\Omega_F/F)$ 叫作 F 的 Brauer 群, 并且表示成 $B_r(F)$:

$$B_r(F) = H^2(\Omega_F/F).$$

由于 F 的代数闭包 Ω 本质上是唯一的, 从而 $B_r(F)$ 实际上是只由 F 所决定的不变量. 当 F 是局部域或者是有限次代数数域(以及有限域上单变量代数函数域)的时候, Brauer 群 $B_r(F)$ 有特别重要的数论意义. 下一节中要研究局部域 k 的 Brauer 群 $B_r(k)$ 的结构.

§ A.3 局部域的 Brauer 群

如上所述,令 k 为局部域, Ω_k 是 k 的最大 Galois 扩域,由定义可知

$$B_r(k) = H^2(\Omega_k/k).$$

设 $K = k_{ar}$ 是 k 的极大不分歧扩域,则 K/k 是 Abel 扩张,从而

$$k \subseteq K \subseteq \Omega_k.$$

于是由引理 5 得出正合序列

$$0 \rightarrow H^2(K/k) \rightarrow B_r(k) \rightarrow B_r(K). \quad (5)$$

让我们首先考查 $H^2(K/k)$.

由 § 3.2 和 § 4.2 可知,对于每个自然数 $n \geq 1$, k 上存在唯一的 n 次不分歧扩张 k_n , 并且

$$K = k_{ar} = \bigcup_{n \geq 1} k_n.$$

设 φ 为 K/k 的 Frobenius 自同构,令 $\varphi_n = \varphi|_{k_n}$, 则

$$G_n = \text{Gal}(k_n/k)$$

是由 φ 生成的 n 阶循环群,从而由引理 4 给出

$$H^2(K/k) = \varinjlim H^2(G_n, k_n^\times),$$

另一方面,从引理 2 可知 φ_n 定义出同构

$$H^2(G_n, k_n^\times) \simeq k_n^\times / N(k_n/k). \quad (6)$$

如果 U 为 k 的单位群而 π 是 k 的素元,则由 § 3.3, 引理 4 可知

$$NU(k_n/k) = U, \quad N(k_n/k) = \langle \pi^n \rangle \times U.$$

由于 k 的正规赋值 v 定义出同构

$$v: k^\times / U \simeq \mathbf{Z},$$

它又诱导出

$$k^\times / N(k_n/k) \simeq \mathbf{Z} / n\mathbf{Z}.$$

从而 $\frac{1}{n} \cdot v$ 给出

$$k^\times / N(k_n/k) \simeq \frac{1}{n} \mathbf{Z} / \mathbf{Z},$$

将同构(6)与上面的同构合成,便定义出

$$H^2(G_n, k_n^\times) \simeq \frac{1}{n} \mathbf{Z}/\mathbf{Z}, \quad n \geq 1. \quad (7)$$

由于这个同构很重要,现在我们把这个映射按照定义具体地写出来. 设 x 为 k^\times 中任意元素,对于 $0 \leq i, j < n$, 令

$$z(\varphi_n^i, \varphi_n^j) = \begin{cases} 1, & \text{如果 } i+j < n, \\ x, & \text{如果 } i+j \geq n, \end{cases}$$

则 $z \in Z^2(G_n, k_n^\times)$, 以 c_x 表示 z 在 $H^2(G_n, k_n^\times) = Z^2/B^2$ 中的陪集, 则 $H^2(G_n, k_n^\times)$ 即是由全体这样的 $c_x (x \in k^\times)$ 所构成的, 同构(7)即是由

$$c_x \mapsto \frac{v(x)}{n} \bmod \mathbf{Z}$$

所给出的. 特别若 x 取成 k 中的素元 π , 可知 $H^2(G_n, k_n^\times)$ 即是由 c_π 生成的 n 阶循环群.

如果 $k \subseteq k_m \subseteq k_n$, $m|n$, 则由引理3可知

$$\begin{array}{ccccc} H^2(G_m, k_m^\times) & \simeq & k^\times/N(k_m/k) & \simeq & \mathbf{Z}/m\mathbf{Z} \\ \downarrow \text{inf} & & \downarrow n/m & & \downarrow n/m \\ H^2(G_n, k_n^\times) & \simeq & k^\times/N(k_n/k) & \simeq & \mathbf{Z}/n\mathbf{Z} \end{array}$$

是交换图表, 其中左边两行的映射分别是由 φ_n 和

$$\varphi_m = \varphi|_{k_m} = \varphi_n|_{k_m}$$

所定义的同构. 从而(7)和它对于 k_m 所对应的同构结合而成的图表

$$\begin{array}{ccc} H^2(G_m, k_m^\times) & \simeq & \frac{1}{m} \mathbf{Z}/\mathbf{Z} \\ \downarrow \text{inf} & & \downarrow \\ H^2(G_n, k_n^\times) & \simeq & \frac{1}{n} \mathbf{Z}/\mathbf{Z} \end{array}$$

也是交换的. 其中右边竖线映射是对于 $m|n$, $\frac{1}{m} \mathbf{Z} \subseteq \frac{1}{n} \mathbf{Z}$ 得到的自然单射. 因此, 若将 \mathbf{Q} 的加法群仍记成 \mathbf{Q} , 则由上面的交换图表得出

$$H^2(K/k) \simeq \varinjlim H^2(G_n, k_n^\times) \simeq \varinjlim \frac{1}{n} \mathbf{Z}/\mathbf{Z} = \mathbf{Q}/\mathbf{Z}.$$

从而证明了如下的定理:

定理 2 设 k_{ur} 是局部域 k 的极大不分歧扩域, 则 k_{ur}/k 的 Frobenius 自同构 φ 定义出自然的同构

$$H^2(k_{ur}/k) \cong \mathbf{Q}/\mathbf{Z}.$$

其次考查 $H^2(K) = H^2(\mathbf{Q}_\ell, K)$. 为此取 E 为 k 的任意有限完全分歧 Galois 扩域, 令 $d = [E:k]$. 又设

$$k' = k_d, \quad E' = k'E.$$

由于 E'/k 是 Galois 扩张, 并且根据假定可知 $k' \cap E = k$, 从而

$$\text{Gal}(E'/k) = \text{Gal}(E'/E) \times \text{Gal}(E'/k'). \quad (8)$$

引理 6 E'/k 如上所述, 则

$$k^\times \subseteq N(E'/k').$$

证明 设 π' 是 E 的素元, 由于 E/k 完全分歧, 则

$$\pi = N_{E/k}(\pi') = N_{E'/k}(\pi')$$

是 k 的素元. 从而只需要证明 k 的单位群 U 的每个元素 u 均包含在 $N(E'/k')$ 之中即可. 设 ρ_k 和 $\rho_{k'}$ 分别为 k 和 k' 的基本映射. 令 $\sigma = \rho_k(u)$, 则由 § 6.2, 定理 4 可知

$$\rho_{k'}(u) = \iota_{k'/k}(\sigma).$$

现在如下定义转移映射 $\iota_{k'/k}(\sigma)$: 对于 $u \in U$, 则

$$\sigma = \rho_k(u) = \delta_k(u)^{-1} \in \text{Gal}(k_{ur}/K).$$

σ 到 $\text{Gal}(\mathbf{Q}_\ell/k)$ 的任意扩充仍记成 σ , 则

$$\sigma \in \text{Gal}(\mathbf{Q}_\ell/K) \subseteq \text{Gal}(\mathbf{Q}_\ell/k').$$

其次, 由于 $k' \cap E = k$, 若令 φ' 是 E_{ur}/E 的 Frobenius 自同构, 则 $\varphi = \varphi'|_K$ 是 K/k 的 Frobenius 自同构, 将 φ' 到 $\text{Gal}(\mathbf{Q}_\ell/E)$ 的扩充仍记成 φ' , 则 $1, \varphi', \dots, \varphi'^{d-1}$ 是 $\text{Gal}(\mathbf{Q}_\ell/k)/\text{Gal}(\mathbf{Q}_\ell/k')$ 的完全代表系, 现在对于 $\sigma \in \text{Gal}(\mathbf{Q}_\ell/k')$, 令

$$\iota_{k'/k}(\sigma) = \left(\prod_{i=0}^{d-1} \varphi'^i \sigma \varphi'^{-i} \right) \Big|_{k'_{ur}}.$$

由于 $\varphi|_{E'} \in \text{Gal}(E'/E)$, $\sigma|_{E'} \in \text{Gal}(E'/k')$ 从 (8) 式可知 $\varphi|_{E'}$ 和 $\sigma|_{E'}$ 是交换的. 因此由上面等式和 $[E':k'] = [E:k] = d$, 得到

$$\iota_{k'/k}(\sigma) \mid E' \cap k'_{ab} = \sigma^d \mid E' \cap k'_{ab} = 1.$$

即

$$\rho_{k'}(u) \mid E' \cap k_{ab} = 1.$$

从而由 § 6.3, 定理 7 和定理 8 的系可知

$$u \in N(E' \cap k'_{ab} / k') = N(E' / k').$$

这就证明了引理.

设 L 是 K 上任意有限 Galois 扩域, 令 $L = K(\alpha)$, α 是 $K[X]$ 中不可约多项式 $f(X)$ 的根. 由于 L/K 是 Galois 扩张, 从而 $f(X)$ 的全部根 $\alpha = \alpha_1, \dots, \alpha_d$ 均属于 L . 因此 $\alpha_i = g_i(\alpha)$, $g_i(X) \in K[X]$, $1 \leq i \leq d$. 由于 $K = k_{ur}$ 为 $k_n (n \geq 1)$ 的并集合, 从而可以唯一决定一个充分大的 n_0 , 使得对于 n_0 的每个倍数 n , $f(X), g_1(X), \dots, g_d(X)$ 的所有系数均属于 k_n . 对于这样的 n 令

$$E = k_n(\alpha),$$

则 E/k_n 是 Galois 扩张, 从而

$$E \cap K = k_n, EK = L,$$

$$\text{Gal}(E/k_n) = \text{Gal}(L/K).$$

定理 3 设 L 是 $K = k_{ur}$ 的任意有限 Galois 扩域, 则

$$N_{L/K}(L^\times) = K^\times.$$

证明 对于上述的 $n \geq 1$, 取 $E = k_n(\alpha)$, 则 E/k_n 是完全分岐 Galois 扩张. 由于 $K = k_{ur} = (k_n)_{ur}$, 将引理 6 用于 K/k_n 和 E/k_n , 令 $E' = k_{nd}E$, 则

$$k_n^\times \subseteq N(E'/k_{nd}).$$

又由 $E \cap K = k_n, EK = L$, 直接得出

$$E \cap K = k_{nd}, E'K = L, \text{Gal}(E'/k_{nd}) = \text{Gal}(L/K),$$

从而由上面得到

$$k_n^\times \subseteq N(E'/k_{nd}) \subseteq N_{L/K}(L^\times).$$

由于 K 是 $\{k_n \mid n \mid n_0\}$ 的并集合, 于是即证明了定理的等式.

本定理和它前面的引理 6 事实上是本节中最重要的结果, 由上述的说明, 可知它可由第六章中所述的局部类域论中的结果

来证明. 注意定理 3 与 § 2.1, 定理 1 类似, 但是 $K = k_{ur}$ 是不完备的.

定理 4 设 k_{ur} 是局部域 k 的极大不分歧扩域, 则

$$B_r(k_{ur}) = H^2(\Omega_r/k_{ur}) = 0.$$

证明 由于 Ω_r 是 $K = k_{ur}$ 上全部有限 Galois 扩域 L 的并集, 从而由引理 4 可知

$$H^2(\Omega_r/K) = \varinjlim H^2(L/K).$$

由上述可知只要对于这样的 L/K 证明 $H^2(L/K) = 0$ 即可. 根据定理 3 前面的注记可知, 对于充分大的 n 令 $k' = k_n$, 则存在有限 Galois 扩张 $E'/k(E = k_n(\alpha))$, 使得

$$E \cap K = k', EK = L, \text{Gal}(E/k') = \text{Gal}(L/K).$$

由于 k' 是局部域, 从 § 3.2, 定理 6 可知 E/k' 是可解扩张. 从而有扩域塔:

$$k' = F_0 \subset F_1 \subset \cdots \subset F_s = E,$$

使得 F_i/F_{i-1} ($1 \leq i \leq s$) 均是循环扩张. 如果令 $M_i = KF_i$ ($0 \leq i \leq s$), 显然有

$$K = M \subset M_1 \subset \cdots \subset M_s = L,$$

其中 $M_i = (F_i)_{ur}$, 并且 M_i/M_{i-1} ($1 \leq i \leq s$) 均是循环扩张. 由引理 2 和定理 3 可知

$$H^2(M_i/M_{i-1}) \simeq M_{i-1}^\times / N_{M_i/M_{i-1}}(M_i^\times) = 0 \quad (1 \leq i \leq s).$$

于是反复使用引理 5 即得到

$$H^2(L/K) = H^2(M_s/M_0) = 0.$$

以上是从定理 3 推导出定理 4. 反过来, 如果假定定理 4 对于每个局部域 k 均成立, 则对于上面的 $M_{i-1} = (F_{i-1})_{ur}$ 有

$$B_r(M_{i-1}) = H^2(\Omega_r/M_{i-1}) = 0.$$

于是由引理 5 得出 $H^2(M_i/M_{i-1}) = 0$, 又由引理 2 可知

$$N_{M_i/M_{i-1}}(M_i^\times) = M_{i-1}^\times \quad (1 \leq i \leq s),$$

从而

$$N_{L/K}(L^\times) = N_{M_s/M_0}(M_s^\times) = M_0^\times = K^\times,$$

这就证明了定理 3. 由此可知, 定理 3 和定理 4 本质上是等价的.

由定理 2, 4 和引理 5 立刻推出如下结果, 这也是本节的主要目标:

定理 5 设 k_{ur} 是局部域 k 的极大不分歧扩域, 则

$$\text{inf}: H^2(k_{ur}/k) \xrightarrow{\sim} H^2(\mathcal{O}_r/k) = \text{Br}(k).$$

从而存在自然的同构

$$\text{Br}(k) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}.$$

对于 $\text{Br}(k)$ 中任意元素 c , 以

$$\text{inv}(c)$$

表示 c 在 $\text{Br}(k) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}$ 之下的象, 即

$$\text{inv}: \text{Br}(k) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}.$$

c 由 $\text{inv}(c)$ 所唯一的决定.

现在设 k' 是 k 的任意有限可分扩域, 则

$$k \subseteq k' \subseteq \mathcal{O}_r,$$

从而可以定义限制映射

$$\text{res}: \text{Br}(k) = H^2(\mathcal{O}_r/k) \rightarrow \text{Br}(k') = H^2(\mathcal{O}_r/k').$$

定理 6 如果 $d = [k': k]$, 则图表

$$\begin{array}{ccc} \text{Br}(k) & \xrightarrow{\sim} & \mathbf{Q}/\mathbf{Z} \\ \downarrow \text{res} & & \downarrow d \\ \text{Br}(k') & \xrightarrow{\sim} & \mathbf{Q}/\mathbf{Z} \end{array}$$

是交换的. 其中行映射均是同构 inv .

证明 设 $e = e(k'/k)$, $f = f(k'/k)$, 令 φ, φ' 分别为 k_{ur}/k 和 k'_{ur}/k' 的 Frobenius 自同构, ν 和 ν' 分别是 k 和 k' 的正规赋值, 则

$$ef = d, \nu'|k = e\nu, \varphi'|k = \varphi'.$$

由于 $\text{Br}(k_{ur}) = H^2(\mathcal{O}_r/k_{ur}) = 0$, 从而由引理 5 后面的注记可知

$$\text{Br}(k) = H^2(k_{ur}/k) = \bigcup_{n \geq 1} H^2(k_n/k).$$

对于 $\text{Br}(k')$ 也有同样的结果. 对于 $c \in \text{Br}(k)$, 则有 $f|n$, $c \in H^2(k_n/k)$. 由同构 (7) 后面的注意可知 $c = c_x$, $x \in k^\times$. 从而 $\varphi_n = \varphi|k_n$, 而 $0 \leq i, j \leq n$ 时, c 是以下面定义的 x 为代表元:

$$z(\varphi_n^i, \varphi_n^j) = \begin{cases} 1, & \text{如果 } i+j < n, \\ x, & \text{如果 } i+j \geq n. \end{cases}$$

因此若令

$$n' = \frac{n}{f}, \quad \varphi_{n'}^{i'} = \varphi_n^i|_{k'},$$

则 $\varphi'|_k = \varphi'$, 于是由限制映射的定义可知 $\text{res}(c)$ 作为 $H^2(k'/k)$ 中元素以满足下面条件的 z' 为代表元, 即对于 $0 \leq i, j \leq n'$ 令

$$z'(\varphi_{n'}^{i'}, \varphi_{n'}^{j'}) = \begin{cases} 1, & i+j < n', \\ x, & i+j \geq n'. \end{cases}$$

再由(7)式后面的注记可知

$$\text{inv}(c) = \frac{v(x)}{n} \bmod \mathbf{Z}, \quad \text{inv}(\text{res}(c)) = \frac{v'(x)}{n'} \bmod \mathbf{Z}.$$

从而

$$\frac{v'(x)}{n'} = \frac{ev(x)}{n'} = ef \frac{v(x)}{n} = d \frac{v(x)}{n},$$

于是得到

$$\text{inv}(\text{res}(c)) = d \text{ inv}(c),$$

这就证明了定理。

在上面定理中, 特别令 k'/k 是 Galois 扩张, 则由引理 5 可知 $H^2(k'/k)$ 可以考虑成是 $\text{res}: \text{Br}(k) \rightarrow \text{Br}(k')$ 的核, 由定理知道 $\text{inv}: \text{Br}(k) \simeq \mathbf{Q}/\mathbf{Z}$ 诱导出自然同构

$$\text{inv}: H^2(k'/k) \simeq \frac{1}{d} \mathbf{Z}/\mathbf{Z}.$$

它是(7)式的推广。

满足

$$\text{inv}(c) = \frac{1}{d} \bmod \mathbf{Z}$$

的元素 $c \in H^2(k'/k)$ 叫作扩张 k'/k 的基本类。由定理 5 和 6 可以对于局部域定义类构造, 用上面的基本类还可以证明 Tate 定理。但是用上同调方法来详细讲述局部类域论并不是我们的目的, 所以就此搁笔。

参 考 文 献

- [1] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York-London-Paris, 1967.
- [2] E. Artin und H. Hasse, Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n -ten Potenzreste im Körper der l^n -ten Einheiten Wurzeln, *Abh. Math. Sem. Hamburg*, 6(1928), 146-162.
- [3] J. W. S. Cassels and A. Fröhlich (edd.), *Algebraic Number Theory*, Thompson Book Co., Washington, D. C., 1967.
- [4] A. Fröhlich, *Formal Groups*, Springer-Verlag, New York-Heidelberg-Berlin, 1968.
- [5] 藤崎源二郎, 体と Galois 理論(岩波講座, 基礎数学), 岩波書店, 1978.
- [6] M. Hazewinkel, Local class field theory is easy, *Advances in Math.*, 16(1975), 147-181.
- [7] 彌永昌吉(編), 数論, 岩波書店, 1969.
- [8] 河田敬義, 代数的整数論, 矢立出版株式会社, 1957.
- [9] J. Lubin and J. Tate, Formal complex multiplication in local fields, *Ann. Math.*, 81(1965), 380-387.
- [10] J. Milnor, *Introduction to algebraic K-theory*, Princeton University Press, Princeton, 1971.
- [11] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1962.
- [12] J.-P. Serre, Sur les corps locaux à corps résiduel algébriquement clos, *Bull. Soc. Math. France*, 89(1961), 105-154.
- [13] B. L. van der Waerden, *Algebra I, II*(sechste Aufl.), Springer-Verlag, New York-Heidelberg-Berlin, 1964.
- [14] A. Weil, *Basic Number Theory* (3rd ed.), Springer-Verlag, New York-Heidelberg-Berlin, 1974.
- [15] A. Wiles, Higher explicit reciprocity laws, *Ann. Math.*, 107(1978), 235-254.